УДК 004.056

Мамедов Мурад Фирдовсиевич

студент, Санкт-Петербургский государственный университет телекоммуникаций им. проф. Бонч-Бруевича

Россия, г. Санкт-Петербург

РАЗРАБОТКА ПРОГРАММНОГО СРЕДСТВА АВТОМАТИЗИРОВАННОГО ФОРМИРОВАНИЯ ПОЛИТИКИ РАЗГРАНИЧЕНИЯ ДОСТУПА В ЛОКАЛЬНОЙ ВЫЧИСЛИТЕЛЬНОЙ СЕТИ МЕДИЦИНСКОЙ ОРГАНИЗАЦИИ

Аннотация. Рассматривается задача автоматизации формирования политики разграничения доступа в сегментированной локальной вычислительной сети медицинской организации. Актуальность работы обусловлена необходимостью защиты персональных данных, медицинской информации и ограничения избыточных сетевых разрешений между различными VLAN-сегментами. Предложено программное средство MedACL Builder, позволяющее создавать сегменты, задавать VLAN и IPv4-подсети, формировать матрицу доступа, добавлять сервисные правила, генерировать ACL и выявлять потенциально опасные политики. Решение может использоваться при предварительном проектировании, настройке и аудите сетевой безопасности медицинских организаций.

Ключевые слова: информационная безопасность, медицинская организация, локальная вычислительная сеть, VLAN, список контроля доступа, ACL, политика разграничения доступа, сегментация сети, Python, MedACL Builder.

Abstract. This paper addresses the problem of automating the creation of access control policies in a segmented local area network at a healthcare organization. The relevance of this work stems from the need to protect personal

data and medical information, as well as to restrict excessive network permissions between different VLAN segments. The MedACL Builder software tool is proposed, which allows users to create segments, specify VLANs and IPv4 subnets, generate an access matrix, add service rules, generate ACLs, and identify potentially dangerous policies. This solution can be used during the preliminary design, configuration, and audit of network security for healthcare organizations.

Keywords: information security, medical organization, local area network, VLAN, access control list, ACL, access control policy, network segmentation, Python, MedACL Builder.

Введение. В условиях цифровизации здравоохранения локальные вычислительные сети медицинских организаций обеспечивают обмен данными между рабочими местами персонала, серверными ресурсами и специализированными информационными системами. При этом в таких сетях обрабатываются персональные данные и сведения о состоянии здоровья граждан, а требования к их защите устанавливаются как общими нормами о персональных данных, так и специальными нормами, связанными с врачебной тайной и защитой информации в ИСПДн [1–4]. В этих условиях задача корректного разграничения сетевого доступа между сегментами становится не только эксплуатационной, но и организационно-технической задачей информационной безопасности. Ручное формирование правил межсегментного взаимодействия на сетевом оборудовании удобно лишь для небольших схем. При увеличении числа VLAN, подсетей и сервисных исключений возрастает вероятность избыточных разрешений, противоречий в правилах и ошибок при переносе политики в ACL. Поэтому актуальной является разработка программного средства, позволяющего формализовать описание сегментов сети и автоматически получать согласованный набор правил доступа по заданной модели.

Постановка задачи. Целью работы является разработка программного средства MedACL Builder для автоматизированного формирования политики разграничения доступа в ЛВС медицинской организации. Программа должна обеспечивать описание сегментов сети по их имени, VLAN, IPv4-подсети и типу зоны; формирование матрицы доступа между сегментами; учёт сервисных правил; генерацию расширенных именованных ACL; а также выявление потенциально опасных разрешений. В качестве адресной основы рассматриваются типовые приватные IPv4-сети, используемые во внутренних инфраструктурах предприятий [5].

Описание архитектуры и реализации. Программа MedACL Builder реализована на языке Python с использованием библиотеки tkinter, которая в официальной документации Python рассматривается как стандартный интерфейс Python к Tcl/Tk [6]. Логика приложения включает модуль описания сегментов, модуль матрицы доступа, модуль сервисных исключений, генератор ACL и модуль формирования отчёта. Пользователь задаёт перечень сегментов сети, для каждого из которых указываются номер VLAN, IPv4-подсеть и тип зоны, например: пользовательская, серверная, административная, гостевая или доверенная. После этого формируется матрица разрешённых и запрещённых взаимодействий между сегментами, а поверх базовой матрицы могут быть заданы сервисные правила для отдельных протоколов и портов.

Таблица 1.

Сравнение ручного и автоматизированного формирования политики доступа

Параметр	Ручная настройка	MedACL Builder
Описание сегментов	Разрозненно в заметках и конфигурациях	В единой структуре: VLAN, подсеть, тип зоны

Формирование правил	По одному правилу вручную	Автоматически по матрице доступа и сервисным исключениям
Проверка рисков	Зависит от внимательности администратора	Выявляются потенциально опасные разрешения и формируется отчет

Методика формирования матрицы доступа и ACL. В основе работы программы лежит формализация политики доступа в виде матрицы, где для каждой пары сетевых сегментов задаётся разрешение или запрет взаимодействия. Далее матрица дополняется сервисными правилами, описывающими допустимые сетевые сервисы, например DNS, HTTPS или иные протоколы, необходимые для работы прикладных систем. Генератор ACL последовательно обрабатывает разрешённые пары сегментов, преобразует их в правила вида «источник — назначение — протокол — порт», после чего формирует итоговый набор расширенных именованных списков доступа. Если в процессе анализа обнаруживаются разрешения из недоверенных или гостевых сегментов в серверные и административные зоны, слишком широкие правила или логические противоречия между матрицей и сервисными исключениями, программа отмечает такие случаи как потенциально опасные.

Результаты на кратком примере. Для иллюстрации работы программы была рассмотрена схема, включающая сегменты «Регистратура», «Врачи», «Серверы» и «Гостевая сеть». В базовой политике доступ из сегментов сотрудников к серверному сегменту разрешается только по необходимым сервисам, тогда как доступ из гостевого сегмента во внутренние зоны запрещается. После задания структуры сегментов и матрицы доступа программа автоматически сформировала набор ACL и одновременно выявила как потенциально опасный сценарий правило, допускающее обращение из гостевой зоны к серверной подсети. Тем самым

MedACL Builder не только ускоряет подготовку конфигурации, но и снижает вероятность сохранения ошибочных разрешений в итоговой политике. В прикладных работах по безопасности корпоративных сетей и передаче результатов аудита также подчёркивается значимость формализованных процедур контроля и систематизации сетевых решений [7, 8].

Заключение. Разработанное программное средство MedACL Builder позволяет автоматизировать формирование политики разграничения доступа в локальной вычислительной сети медицинской организации и сократить число ошибок, характерных для ручной подготовки ACL. Практическая применимость решения связана с задачами предварительного проектирования, внутреннего аудита и подготовки согласованных правил доступа для сегментированных сетей, в которых обрабатываются персональные данные и медицинская информация. Ограничением текущей версии является ориентация на заранее заданную модель сегментов и сервисных правил без автоматического получения топологии из сетевого оборудования. Дальнейшее развитие программы может быть связано с поддержкой нескольких синтаксисов ACL, импортом конфигураций и расширением набора проверок на логические конфликты политики.

СПИСОК ЛИТЕРАТУРЫ

1. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_61801/ (дата обращения: 02.07.2026).
2. Постановление Правительства Российской Федерации от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_137356/ (дата обращения: 02.07.2026).

3. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. URL: https://fstec.ru/dokumenty/vse-dokumenty/spetsialnye-normativnye-dokumenty/prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 02.07.2026).
4. Федеральный закон от 21.11.2011 № 323-ФЗ «Об основах охраны здоровья граждан в Российской Федерации» [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_121895/ (дата обращения: 02.07.2026).
5. Rekhter Y., Moskowitz B., Karrenberg D., de Groot G. J., Lear E. Address Allocation for Private Internets: RFC 1918 [Электронный ресурс]. URL: https://www.rfc-editor.org/rfc/rfc1918 (дата обращения: 02.07.2026).
6. Python Software Foundation. tkinter — Python interface to Tcl/Tk // Python Documentation [Электронный ресурс]. URL: https://docs.python.org/3/library/tkinter.html (дата обращения: 02.07.2026).
7. Махмутова Н. Ф., Бирих Э. В., Сахаров Д. В. Исследование способов повышения безопасности корпоративных сетей // Вестник Дагестанского государственного технического университета. Технические науки. 2024. Т. 51. № 3. С. 110–116.
8. Костарев С. В., Липатников В. А., Сахаров Д. В. Модель процесса передачи результатов аудита и контроля в автоматизированной системе менеджмента предприятия интегрированной структуры // Проблемы информационной безопасности. Компьютерные системы. 2015. № 2. С. 120–125.