УДК 004.72:004.56

# МЕТОД ПРЕДОТВРАЩЕНИЯ УГРОЗ В ЗАКРЫТОЙ СЕТЕВОЙ ИНФРАСТРУКТУРЕ НА ОСНОВЕ ВНУТРЕННЕЙ СЕГМЕНТАЦИИ

В.В. Чиж
*Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь*

**Аннотация.** Предложен метод предотвращения распространения вредоносного кода в закрытой сетевой инфраструктуре на основе внутренней сегментации и внутренних сегментирующих межсетевых экранов (*Internal Segmentation Firewall*, *ISFW*). Сеть делится на изолированные сегменты безопасности с централизованным управлением доступов. Контроль трафика позволяет ограничить латеральное перемещение атакующего при компрометации одного узла. Приводится упрощенная модель оценки вероятности успешного распространения атаки и текстовое описание блок-схемы закрытой сетевой инфраструктуры.
**Ключевые слова:** закрытая сеть; межсетевой экран; латеральное перемещение; модель угроз.

# METHOD FOR PREVENTING THREATS IN A CLOSED NETWORK INFRASTRUCTURE BASED ON INTERNAL SEGMENTATION

V.V. Chizh
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

**Abstract.** A method for preventing the spread of malicious code in a closed network infrastructure based on internal segmentation and Internal segmentation firewalls (ISFW) is being considered. The network is divided into isolated security segments with centralized access control. Traffic control allows you to limit the lateral movement of an attacker when one node is compromised. A simplified model for estimating the probability of successful spread of an attack and a text description of a block diagram of a closed network infrastructure are provided.
**Keywords:** closed network; firewall; lateral movement; threat model.

## Введение

Закрытые сетевые инфраструктуры считаются более защищенными из-за отсутствия прямого подключения к интернету, однако многие атаки реализуются через внутренние узлы: ошибки администрирования, уязвимости приложений и компрометацию учетных записей. Для критических систем это создает риск быстрого выхода злоумышленника на серверы управления технологическими процессами и базы данных.

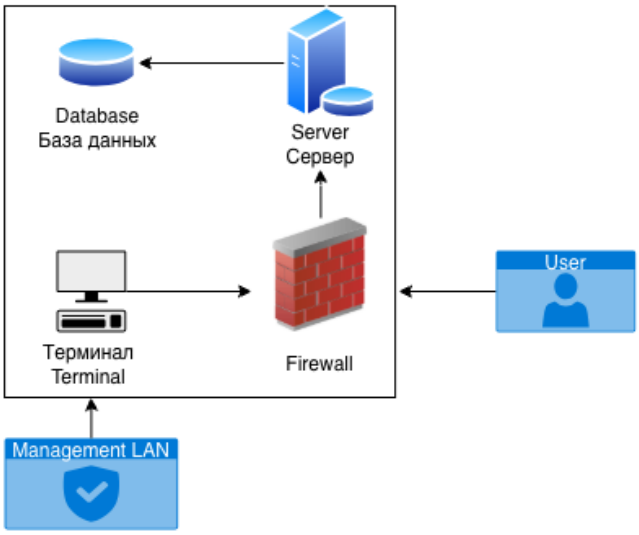
Цель – описать метод предотвращения распространения вредоносного кода в закрытой сети на основе такой сегментации.

## Основная часть

Рассматривается латеральное распространение вредоносного ПО после компрометации одной рабочей станции в офисном сегменте. Цель несанкционированного доступа: получить управление к сегментам, где размещены сервера приложений, базы данных и системы управления. Предполагается логическое разделение сети на несколько подсетей, наличие критических и некритических сегментов, а также отсутствие прямого доступа в интернет при наличии контролируемых шлюзов. Задача защиты – уменьшить вероятность перехода из некритического в критический сегмент без потери необходимой функциональности.

Внутренняя сегментация – это разбиение сети на сегменты безопасности, взаимодействие между которыми разрешено только по заранее определенным правилам. Для реализации используются внутренний сегментирующий межсетевой экран, установленный на стыке виртуальной сети. Он фильтруют межсегментный трафик, применяют анализ пакетов и поведенческое обнаружение вредоносной активности, контролируя трафик не только на периметре, но и между внутренними сегментами.

Упрощенная структура закрытой сети с внутренней сегментацией приведена на рисунке.




Структурная схема закрытой сетевой инфраструктуры с внутренней сегментацией
Block diagram of a closed network infrastructure with internal segmentation

Метод включает: аналитическое выделение сегментов и критических ресурсов; проектирование модели сегментации и точек установки внутренних экранов; организацию централизованного мониторинга и оперативной изоляции подозрительных сегментов [1, 2].

## Заключение

Предложенный метод внутренней сегментации и применения внутренних сегментирующих межсетевых экранов позволяет ограничить распространение вредоносного кода в закрытой сети и снизить вероятность достижения критических сегментов при успешной компрометации одного узла. Упрощенная модель показывает, что увеличение количества контролируемых межсегментных переходов и улучшение качества настроек политик приводит к уменьшению вероятности успешной атаки. Данный подход особенно полезен для сетей критической инфраструктуры и может быть адаптирован под конкретные архитектуры и регуляторные требования.

## Список использованных источников

1. Альравашде К., Перди С. Формальный подход к сегментации сети. Компьютеры и безопасность (2021), 99–102.
2. Ранжирование объектов критической информационной инфраструктуры сотовых сетей. Вестник Алтайской академии экономики и права (2023), 324–334.

## References

1. Alrawashdeh K., Purdy C. A Formal Approach to Network Segmentation. Computers & Security (2021), 99–102.
2. Ranking of objects of critical information infrastructure of cellular networks. Bulletin of the Altai Academy of Economics and Law (2023), 324–334.

## Сведения об авторе

**Чиж В.В.,** магистрант кафедры защиты информации, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», vik220011@gmail.com.

## Information about the author

**Chizh V.,** master's student at the Information Protection Department, Educational Institution "Belarusian State University of Informatics and Radioelectronics", vik220011@gmail.com.