

БЕЛОРУССКИЙ НАЦИОНАЛЬНЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ
Факультет информационных технологий и робототехники
Кафедра «Программное обеспечение информационных систем и технологий»

ДОПУЩЕН К ЗАЩИТЕ

Заведующий кафедрой


Ю.В. Полозков
(инициалы и фамилия)

«04» 06 2025 г.

РАСЧЕТНО-ПОЯСНИТЕЛЬНАЯ ЗАПИСКА
ДИПЛОМНОГО ПРОЕКТА

«Система контроля и фильтрации сетевого трафика»

Специальность 1-40 05 01 «Информационные системы и технологии (по направлениям)»

Направление специальности 1-40 05 01-04 «Информационные системы и технологии (в обработке и представлении информации)»

Обучающийся

группы 10702121
(номер)

Руководитель

Консультанты:

по разделу «Компьютерное проектирование»

по разделу «Охрана труда»

по разделу «Экономика»

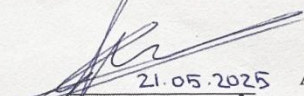
Ответственный за нормоконтроль

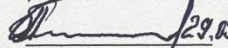
Объем проекта:


расчетно-пояснительная записка – 43 страниц;

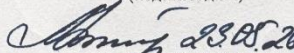
графическая часть – 10 листов;


магнитные (цифровые) носители – 1 единиц.

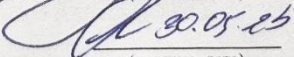

21.05.2025 А.А. Бортник
(подпись, дата)


29.05.25 О.А. Пашкевич
(подпись, дата)


29.05.25 О.А. Пашкевич
(подпись, дата)


23.05.25 М.Л. Калиниченко
(подпись, дата)


29.05.25 О.В. Куневич
(подпись, дата)


30.05.25 Л.В. Федосова
(подпись, дата)

Минск 2025

РЕФЕРАТ

СЕТЕВОЙ ТРАФИК, МОНИТОРИНГ, ФИЛЬТРАЦИЯ,
БЛОКИРОВКА IP, PYTHON, FLASK, SCAPY, IPTABLES,
ПРОЕКТИРОВАНИЕ, РЕАЛИЗАЦИЯ, ТЕСТИРОВАНИЕ

Объектом разработки является система контроля и фильтрации сетевого трафика с функцией автоматического реагирования на подозрительную активность.

Цель проекта - разработать программный продукт, предназначенный для мониторинга входящего/исходящего сетевого трафика, а также фильтрации и блокировки нежелательных подключений в автоматическом и ручном режимах.

Областью практического применения является обеспечение сетевой безопасности в организациях, учебных заведениях и на индивидуальных рабочих станциях. Система позволяет отслеживать сетевую активность в реальном времени, оперативно выявлять подозрительное поведение (например, чрезмерное количество пакетов от одного источника), автоматически блокировать такие подключения и вести журнал трафика. Это способствует снижению рисков несанкционированного доступа, DDoS-атак и утечек информации.

Студент-дипломник подтверждает, что все технические решения, методы реализации и приведённые в проекте материалы достоверно отражают процесс разработки системы. Используемые компоненты, включая библиотеки Python (scapy, subprocess, sqlite3) и механизмы управления трафиком Linux (iptables), задокументированы с опорой на официальную документацию и профильные ресурсы в области информационной безопасности.

Дипломный проект: 49 с., 11 рис., 9 табл., 12 источников, 1 прил.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

- 1 Сейц Дж. Black Hat Python: Python для хакеров и пентестеров. – М.: ДМК Пресс, 2015. – 192 с.
- 2 Таненбаум Э. Современные операционные системы. – СПб.: Питер, 2019. – 1120 с.
- 3 Безопасность компьютерных сетей: Основы защиты информации. – М.: ДМК Пресс, 2021. – 368 с.
- 4 Скамбрэй Дж. Хакерские атаки: Искусство эксплуатации. – М.: ДМК Пресс, 2011. – 512 с.
- 5 Кауфман Ч., Перлман Р., Спек М. Сетевое обеспечение безопасности: IPsec, VPN и приложения. – СПб.: Питер, 2018. – 768 с.
- 6 Аллен Дж. Безопасность информационных систем. – М.: Вильямс, 2017. – 640 с.
- 7 Шнайер Б. Прикладная криптография. Протоколы, алгоритмы и исходные тексты на языке Си. – М.: Триумф, 2016. – 816 с.
- 8 Zeltser L. Malware Analysis and Incident Response Techniques. – SANS Institute, 2020. – 350 p.
- 9 Журавлев А.В., Иванов С.А. Анализ сетевого трафика с использованием Scapy. – М.: Директ-Медиа, 2020. – 224 с.
- 10 Олифер В.Г., Олифер Н.А. Сетевые технологии. – М.: БХВ-Петербург, 2021. – 864 с.
- 11 Документация по библиотеке Scapy. – [Электронный ресурс]. – Режим доступа: <https://scapy.readthedocs.io>
- 12 Документация по iptables – [Электронный ресурс]. – Режим доступа: <https://netfilter.org/projects/iptables>