

МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ
БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ФАКУЛЬТЕТ РАДИОФИЗИКИ И КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ
Кафедра телекоммуникаций и информационных технологий

КРАСИЛЬНИКОВА
Мария Алексеевна

**АВТОМАТИЧЕСКОЕ РАЗВЕРТЫВАНИЕ В DOCKER-
КОНТЕЙНЕРАХ УЯЗВИМЫХ ОПЕРАЦИОННЫХ СИСТЕМ
ДЛЯ КИБЕРПОЛИГОНА**

Аннотация к дипломной работе

Научный руководитель – старший преподаватель А.М. Соболев

Минск, 2023

РЕФЕРАТ

Дипломная работа: 66 с., 24 рис., 18 источников.

КОНТЕЙНЕРИЗАЦИЯ, ВИРТУАЛИЗАЦИЯ, РАЗРАБОТКА ПРИЛОЖЕНИЯ, DOCKER, PYTHON

Объект исследования – Docker-контейнеры и уязвимости.

Цель работы – разработка методики автоматического развертывания уязвимых операционных систем в Docker-контейнерах для использования на киберполигонах.

В процессе выполнения дипломной работы были проанализированы технологии контейнеризации и виртуализации. Также были изучены распространенные уязвимости операционных систем Windows и Linux. Для создания уязвимых Docker-образов были настроены файлы Dockerfile и docker-compose.yml. Кроме того, были разработаны требования и реализована модель автоматического развертывания Docker-контейнеров для использования на киберполигонах.

РЭФЕРАТ

Дыпломная праца: 67 с., 24 мал., 18 крыніц.

КАНТЭЙНЕРЫЗАЦЫЯ, ВІРТУАЛІЗАЦЫЯ, РАСПРАЦОЎКА ДАДАТКІ, DOCKER, PYTHON

Аб'ект даследавання – Docker-кантэйнеры і ўразлівасці.

Мэта працы – распрацоўка метадыкі аўтаматычнага разгортвання ўразлівых аперацыйных сістэм у Docker-кантэйнерах для выкарыстання на кіберпалігонах.

У працэсе выканання дыпломнай працы былі прааналізаваны тэхналогіі кантэйнерызацыі і віртуалізацыі. Таксама былі вывучаны распаўсюджаныя ўразлівасці аперацыйных сістэм Windows і Linux. Для стварэння ўразлівых Docker-вобразаў былі наладжаны файлы Dockerfile і docker-compose.yml. Акрамя таго, былі распрацаваны патрабаванні і рэалізавана мадэль аўтаматычнага разгортвання Docker-кантэйнераў для выкарыстання на кіберпалігонах.

ABSTRACT

The degree work: 67 pages, 24 pictures, 18 sources.

**CONTAINERIZATION, VIRTUALIZATION, APP DEVELOPMENT,
DOCKER, PYTHON**

The object of research is Docker containers and vulnerabilities.

The purpose of the work is to develop a methodology for automatically deploying vulnerable operating systems in Docker containers for use in cyber training grounds.

During the course of the diploma work, containerization and virtualization technologies were analyzed, as well as common vulnerabilities in Windows and Linux operating systems. Dockerfile and docker-compose.yml have been configured to create vulnerable Docker images. To create vulnerable Docker images, Dockerfile and docker-compose.yml files were configured. Additionally, requirements were developed and a model for automatic deployment of Docker containers for use in cyber training grounds was implemented.