**САНКТ-ПЕТЕРБУРГСКИЙ ПОЛИТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ПЕТРА ВЕЛИКОГО**

**Институт компьютерных наук и кибербезопасности**

**Высшая школа кибербезопасности**

**РЕКОМЕНДАЦИИ**

**по оформлению выпускной квалификационной работы**

Санкт-Петербург ⸻ 2023

 Общие требования к структуре ВКР

Структура выпускной квалификационной работы включает следующие разделы:

1. **Титульный лист** (оформляется согласно установленному шаблону, представленному в Приложении 1).
2. **Реферат** (пример оформления представлен в Приложении 2). Реферат должен быть выполнен на двух языках (русском и английском) и содержать:
* предмет, тему, цель ВКР;
* метод или методологию проведения ВКР;
* результаты ВКР;
* область применения результатов ВКР;
* выводы.

Ограничения на объем реферата на русском языке − от 1000 до 1500 печатных знаков. Страницы с рефератом не нумеруются.

1. **Содержание** включает в себя наименование всех разделов, подразделов с указанием номеров страниц до заголовков третьего уровня включительно (см. Приложение 3). Нумерация разделов, подразделов выполняется с помощью арабских цифр. Введение, заключение, список использованных источников, приложения в содержании не нумеруются. Отдельные элементы содержания отделяют друг от друга одинарным интервалом.
2. **Определения, обозначения и сокращения** содержит перечень обозначений и сокращений, применяемых в тексте ВКР (см. Приложение 4).
3. **Введение** содержит обоснование выбора темы, характеристику современного состояния изучаемой проблемы, ее актуальность, практическую и теоретическую значимость, степень разработанности данной проблемы в России и за рубежом. Во введении не включают схемы, таблицы, описания, рекомендации и т.п. Введение должно содержать следующие аспекты:
* актуальность исследования;
* объект исследования и предмет исследования;
* цель работы и поставленные задачи;
* теоретическую основу ВКР, материалы для практической части ВКР;
* информационную базу исследования;
* степень научной разработанности проблемы;
* научную новизну;
* практическую значимость ВКР;
* апробацию результатов исследования (выступления на научных конференциях, симпозиумах, форумах и т.п., публикации студента, включенные в список использованных источников).
1. **Основная часть ВКР** содержит результаты исследования. Каждый раздел ВКР должен содержать выводы, обобщающие результаты, полученные в рамках данного раздела, с аннотацией следующей части работы. Рекомендуемый объем основной части ВКР – не менее 50 страниц.
2. **Заключение** содержит основные выводы по теме работы, которые соответствуют поставленным задачам. Объем заключения не должен превышать двух страниц.
3. **Список использованных источников** является обязательной частью выпускной квалификационной работы. Список должен включать не менее 20 источников. Оформление источников выполняется в соответствии с требованиями ГОСТ Р 7.0.5-2008 «Система стандартов по информации, библиотечному и издательскому делу. Библиографическая ссылка. Общие требования и правила составления». Сведения об источниках следует располагать в порядке появления ссылок на источники в тексте ВКР и нумеровать арабскими цифрами, выделенными квадратными скобками (например, [1], [2−4]).
4. **Приложения** представляют собой вспомогательный материал, имеющий справочное значение или дополняющий основной текст ВКР. По форме это может быть текст, таблицы, графики, программный код, описание алгоритмов и т.п. На приложения даются ссылки в основном тексте ВКР; обозначение приложения осуществляется с помощью арабских цифр (например: в Приложении 1 приведен алгоритм программы). Каждое приложение должно начинаться с новой страницы с указанием в правом верхнем углу слова «Приложение» и иметь тематический заголовок. Общий объём приложений не должен превышать 20% от объёма основного текста ВКР.

Требования к оформлению ВКР

Текст ВКР оформляется в формате А4, шрифтом Times New Roman, кегль 14, с междустрочным интервалом 1,5 и полями: левое – 30 мм, правое – 10 мм, верхнее и нижнее – 20 мм. Абзацный отступ – 1,25 см. Нумерация страниц – вверху страницы справа на уровне 10 мм от края листа арабскими цифрами.

Текст должен быть выровнен по ширине страницы, в нем должны быть сделаны переносы (переносы не допускаются только в названиях разделов, подразделов и т.п.). Рекомендуется избегать полупустых страниц, висячих строк.

Введение, заключение, список использованных источников и приложения начинают с новой страницы. Заголовки **ВВЕДЕНИЕ,** **СОДЕРЖАние, ЗАКЛЮЧЕНИЕ, СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ** пишутся заглавными буквами, полужирным шрифтом, кегль 14, центрованным способом на границе верхнего поля. Затем отступается удвоенный интервал (пропущенная строка) и печатается само содержимое.

Каждый раздел основной части ВКР также начинается с новой страницы; подразделы и заголовки следующих уровней печатаются подряд, с соблюдением интервалов, например:

# Название раздела

Заголовки разного уровня оформляются разными способами с изменением выделения. Пример оформления разделов и подразделов. Перед названием каждого подраздела ставится пустая строка.

## Первый подраздел

Для оформления названия заголовков используйте соответствующие стили, представленные в этом документе. Все заголовки выровнены посередине. После названия раздела точка не ставится.

### Пример заголовка третьего уровня

Рисунки должны иметь номер и название и могут иметь поясняющие надписи. Рисунки нумеруют в пределах раздела, например, рисунок 2.3 – третий рисунок второй главы. Если в работе только один рисунок, то его не нумеруют.

На каждый рисунок должна быть ссылка в тексте перед самим рисунком (например: как показано на рисунке 2.3, на рисунке 2.3 приведена статистика). Пример оформления рисунков:



Рисунок 1.1 – Статистика роста числа кибератак в 2017 и 2018 гг

Рисунки располагаются по центру, без выступов. После названия рисунка ставится пустая строка с одинарным междустрочным интервалом. Если подрисуночная надпись занимает две строки, то для нее также определяется одинарный междустрочный интервал.

Для оформления горизонтально направленных иллюстраций делается разделение документа на части с помощью разрывов страниц и выбирается альбомная ориентация. Страницы с горизонтальной ориентацией не нумеруются.



Рисунок 1.2 – Пример оформления горизонтально направленной иллюстрации с подрисуночной надписью на двух строках

Листы с альбомной ориентацией имеют следующие поля: верхнее – 30 мм, нижнее – 10 мм, левое и правое – 20 мм.

На таблицы также должны быть ссылки в тексте. Пример: в табл. 1.1 приведена общая статистика по исследуемому набору данных. Номер таблицы соответствует номеру раздела (если в разделе несколько таблиц, то нумерационный заголовок включает номер раздела и порядковый номер таблицы в этом разделе). Перед самой таблицей ставится пустая строка с междустрочным интервалом в 1.

Таблица 1.1 – Результаты проверки средства на тестовом сервере

|  |  |  |
| --- | --- | --- |
|  | Число срабатываний | Среднее время выполнения |
| Обнаружен вызов panic | 41 | 4,3 с |
| Обнаружен вызов kasan\_report | 59 | 4,1 с |
| Завершение тестирования по истечению таймаута | 0 | – |

После таблицы ставится пустая строка с междустрочным интервалом 1,5. внутри таблицы - междустрочный интервал в 1,15. Заголовки выровнены по центру, остальной текст – по левому краю. Рекомендуется обратить внимание на корректный перенос слов в таблице.

Таблица 1.2 – Общая статистика UNSW-NB15 [45] (здесь нет отступа и междустрочный интервал 1)

|  |  |
| --- | --- |
| Общее количество записей | 1964509 |
| Количество исходящих байт | 5454221244 |
| Количество входящих байт | 89046756452 |
| Количество исходящих пакетов | 82298235 |
| Количество входящих пакетов | 105988377 |
| Протокол | TCP | 1492153 |
| UDP | 990144 |
| ICMP | 524 |
| Другой | 524 |
| Метка | Обычный  | 2218761 |
| Вредоносный | 321283 |
| Количество уникальных IP-адресов | 45 |

Если таблица занимает более одного листа, то ее заголовок необходимо дублировать при переносе на другой лист, а в названии добавить слово «продолжение».

Таблица 1.3 – Результаты классификации набора данных

|  |  |
| --- | --- |
| Заголовок 1 | Заголовок 2 |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Таблица 1.3 – Результаты классификации набора данных (продолжение)

|  |  |
| --- | --- |
| Заголовок 1 | Заголовок 2 |
|  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |  |

Код в ВКР можно вставлять в объеме не больше, чем на полстраницы единовременно, выделять другим шрифтом (согласно стилю «Программный код»), обязательно оформляя комментарии, например:

 for i in range (0, len(equation\_inputs)):

 w\_summ += equation\_inputs[i] #подсчет суммы всех весовых коэффициентов

 for i in range (0, k):

 w=0

 new\_fit=0

 for j in range (0, n): #целевая функция

 w += pop[i][j]\*(equation\_inputs[j])

 new\_fit = count1[i]/n + w/w\_summ

 fitness.append(new\_fit)#создание вектора значений целевой функции

Для оформления списков также рекомендуется использовать соответствующие стили. Примеры оформления:

1. Элементы списка обозначены числом с точкой.
2. Поэтому в конце ставится точка.

Для маркировки списков следующего уровня могут быть использованы арабские цифры с круглой скобкой, буквы русского алфавита с круглой скобкой, тире:

1. начинаются с маленькой буквы, в конце точка с запятой;
2. и тут также;
3. а в конце точка.

или

1. один;
2. два;
3. три.

или

* …………;
* …………;
* ………….. .

Не допускается использование иных наборных знаков (квадрат, ромб, звездочка, галочка и т. п.).

Уравнения и формулы не допускается представлять в виде рисунков или текста. Они должны быть выполнены с использованием конструктора формул (например, Microsoft Equation, MathType). Если на формулу в тексте есть ссылка, то ее нумеруют арабскими цифрами в круглых скобках на уровне формулы у правого поля. Например (2.4) − четвертая формула второго раздела. После формулы ставят запятую, а первую строку пояснения начинают словом «где» без двоеточия. В тексте ссылку указывают следующим образом: «… в формуле (2.4)» или «… в (2.4)». Пример оформления формулы:

|  |  |
| --- | --- |
| $$ w\_{x}=\frac{2\*H\_{max}-H\left(x\right)}{2}, если 0.5<P(x=1)\leq 1,$$ | (2.4) |

где $H\left(x\right)- $ энтропия каждого параметра, $H\_{max}$ – максимальное значение энтропии всех параметров, $P\left(x\right)- $вероятность наступления события *x,* $w(x)$ *–* вес параметра *x*.

Если на формулу ссылки в тексте нет, то ее можно не нумеровать. Пример оформления списка использованных источников:

1. Ванцева И. О. Влияние Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» на владельцев критических информационных инфраструктур //Вестник УрФО. Безопасность в информационной сфере. — 2018. — №. 1 (27). — С. 71–76.
2. Cyber Attacks Statistics 2019 [Электронный ресурс]. URL: <https://www.hackmageddon.com/category/security/cyber-attacks-statistics/>. — (дата обращения: 05.01.2020).
3. Naidu N., Dharaskar R. V. An effective approach to network intrusion detection system using genetic algorithm //International journal of computer applications. — 2010. — Vol. 1. — №. 3. — P. 26–32.
4. Браницкий А. А., Котенко И. В. Анализ и классификация методов обнаружения сетевых атак //Труды СПИИРАН. — 2016. — Т. 2. — №. 45. —
С. 207–244.
5. Hua Zhou et al. Application of Support Vector Machine and Genetic Algorithm to Network Intrusion Detection, Wireless Communications, Networking and Mobile Computing 2007, WiCom 2007, 21–25 Sept. 2007. — P. 2267–2269.
6. Системы и методы обнаружения вторжений: современное состояние и направления совершенствования [Электронный ресурс]. URL: <http://citforum.ru/security/internet/ids_overview/>. — (дата обращения: 12.12.2019).
7. Jha J., Ragha L. Intrusion detection system using support vector machine //International Journal of Applied Information Systems (IJAIS). — 2013. — №. 3. — P. 25–30.
8. Платонов В. В., Семёнов П. О. Методы сокращения размерности в системах обнаружения сетевых атак //Проблемы информационной безопасности. Компьютерные системы. — 2012. — №. 3. — С. 40–45.
9. Сайт «Библиотека программиста». [Электронный ресурс]. URL: <https://proglib.io/p/xgboost/>. — (дата обращения: 20.12.2019).
10. Feature Importance and Feature Selection With XGBoost in Python. [Электронный ресурс]. URL: <https://machinelearningmastery.com/feature-importance-and-feature-selection-with-xgboost-in-python/>. — (дата обращения: 25.12.2019).
11. Гэри М., Джонсон Д. Вычислительные машины и труднорешаемые задачи. М.: Мир, 1982. — 419 c.

Обратите внимание как оформляются ссылки на электронные ресурсы.

Заголовок приложения оформляется прописными буквами, выравнивание – по правому краю. Каждое приложение должно иметь название, например:

ПРИЛОЖЕНИЕ 1. НАЗВАНИЕ ПРИЛОЖЕНИЯ

ПРИЛОЖЕНИЕ 1. Примеры оформлений титульных листов

Министерство науки и высшего образования Российской Федерации

Санкт-Петербургский политехнический университет Петра Великого

Институт компьютерных наук и кибербезопасности

Высшая школа кибербезопасности

 Работа допущена к защите

 Директор Высшей школы

кибербезопасности, д.т.н., проф., чл.-корр. РАН

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д.П. Зегжда

 «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2024 г.

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

РАБОТА БАКАЛАВРА

**ТЕМА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**

по направлению подготовки (специальности)

10.03.01 Информационная безопасность

Направленность (профиль)

10.03.01\_03 Безопасность компьютерных систем

Выполнил

студент гр. И.О. Фамилия

Руководитель

должность, ученая степень,

ученое звание И.О. Фамилия

Консультант

должность, ученая степень,

ученое звание И.О. Фамилия

Санкт-Петербург – 2024

Министерство науки и высшего образования Российской Федерации

Санкт-Петербургский политехнический университет Петра Великого

Институт компьютерных наук и кибербезопасности

Высшая школа кибербезопасности

 Работа допущена к защите

 Директор Высшей школы

кибербезопасности, д.т.н., проф., чл.-корр. РАН

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д.П. Зегжда

 «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2024 г.

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

ДИПЛОМНАЯ РАБОТА

**ТЕМА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**

по направлению подготовки (специальности)

10.05.03 Информационная безопасность автоматизированных систем

Направленность (профиль)

10.05.03\_08 Анализ безопасности информационных систем

Выполнил

студент гр. И.О. Фамилия

Руководитель

должность, степень,

звание И.О. Фамилия

Консультант

должность, ученая степень,

ученое звание И.О. Фамилия

Санкт-Петербург – 2024

Министерство науки и высшего образования Российской Федерации

Санкт-Петербургский политехнический университет Петра Великого

Институт компьютерных наук и кибербезопасности

Высшая школа кибербезопасности

 Работа допущена к защите

 Директор Высшей школы

кибербезопасности, д.т.н., проф., чл.-корр. РАН

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Д.П. Зегжда

 «\_\_\_»\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_2024 г.

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ

**ТЕМА ВЫПУСКНОЙ КВАЛИФИКАЦИОННОЙ РАБОТЫ**

по направлению подготовки (специальности)

10.04.01 Информационная безопасность

Направленность (профиль)

10.04.01\_01 Математические методы компьютерной безопасности

Выполнил

студент гр. И.О. Фамилия

Руководитель

должность, степень,

звание И.О. Фамилия

Консультант

должность, ученая степень,

ученое звание И.О. Фамилия

Санкт-Петербург – 2024

ПРИЛОЖЕНИЕ 2. рЕФЕРАТ

**РЕФЕРАТ**

На 60 с., 12 рисунков, 5 таблиц, 6 приложений

КЛЮЧЕВЫЕ СЛОВА: ФАЗЗИНГ, ПОИСК УЯЗВИМОСТЕЙ, ЯДРО LINUX, АППАРАТНАЯ ВИРТУАЛИЗАЦИЯ, СЕТЕВОЙ СТЕК

Тема выпускной квалификационной работы: «Анализ безопасности сетевого стека ядра Linux на основе фаззинга с сохранением состояния».

Целью работы является поиск программных дефектов в сетевом стеке ядра Linux на основе технологии фаззинга с сохранением состояния. Предметом исследования являются современные методы автоматизированного поиска программных дефектов в сетевом стеке ядра Linux. Задачи, решаемые в ходе исследования:

1. Исследование внутреннего устройства сетевого стека ядра Linux.
2. Анализ современных исследований в области поиска программных дефектов в реализации ядра Linux.
3. Разработка метода поиска программных дефектов в сетевом стеке ядра Linux на основе фаззинга с сохранением состояния.
4. Программная реализация разработанного метода.
5. Оценка скорости и точности работы созданного средства.

В ходе работы была исследована архитектура и реализация сетевого стека ядра Linux. Были проанализированы современные исследования в области обеспечения безопасности ядра Linux.

В результате работы было разработано средство поиска программных дефектов в сетевом стеке ядра Linux, была продемонстрирована эффективность средства. Был сделан вывод, что безопасность сетевого стека мало изучена.

Полученные результаты могут быть использованы в качестве основы для проектирования систем динамического анализа сетевого стека ядра Linux.

**ABSTRACT**

60 pages, 12 figures, 5 tables, 6 appendices

KEYWORDS: FUZZING, VULNERABILITY SCANNING, LINUX KERNEL, HARDWARE VIRTUALIZATION, NETWORK STACK

The topic of the graduate qualification work is «Analysis of Linux kernel network stack security based on fuzzing with snapshots».

The purpose of the study is Linux kernel network stack program defect scanning based on fussing with snapshots. The subject of the work is modern automated program defect search methods in Linux kernel network stack. The research set the following goals:

1. Studying inner working of Linux-family OS kernel network stack.
2. Analysis of modern studies on scanning software defects in Linux kernel.
3. Development of method to find software defects in Linux kernel network stack implementation based on fuzzing with snapshots.
4. Software implementation of the developed method.
5. Scanning defect accuracy and speed assessment of the developed software implementation.

During the work Linux kernel network stack implementation and architecture were studied. Modern studies in Linux kernel security and vulnerabilities scanning areas were analyzed.

The work resulted in development of a tool to find Linux kernel network stack software defects. Tool has satisfactory indicators in not only quantitative defect detection, but also in productivity. The studying point to conclusion that Linux kernel network stack security is poorly examined.

The results could be used as a base for dynamic analysis mechanisms designing for Linux kernel network stack.

.

ПРИЛОЖЕНИЕ 3. сОДЕРЖАНИЕ

Содержание

|  |  |  |
| --- | --- | --- |
| Введение......................................................................................................... |  | 6 |
| 1 | Проблемы обнаружения сетевых атак ............................................ |  | 10  |
| 1.1 | Проблема выбора алгоритма обнаружения сетевых атак.............. |  | 10 |
| 1.2 | Проблема формирования исходных данных для обнаружения сетевых атак....................................................................................... |  | 12 |
| 1.3 | Проблема выбора анализируемых параметров трафика ............... |  | 13 |
| 1.4 | Проблема обеспечения высокой точности обнаружения сетевых атак...................................................................................................... |  | 14 |
| 2 | Сокращение количества параметров сетевого трафика................. |  | 16 |
| 2.1 | Методы сокращения размерности.................................................... |  | 16 |
| 2.1.1 | Генетический алгоритм..................................................................... |  | 19 |
| 2.2 | Методы весовых коэффициентов..................................................... |  | 24 |
| 2.2.1 | Энтропийный метод.......................................................................... |  | 24 |
| 2.2.2 | Метод главных компонент................................................................ |  | 25 |
| 3 | Экспериментальные результаты...................................................... |  | 37 |
| 3.1 | Набор данных UNSW-NB15............................................................. |  | 41 |
| 3.2 | Набор данных TrabID 2017............................................................... |  | 51 |
| Заключение.................................................................................................... |  | 54 |
| Список использованных источников.......................................................... |  | 56 |
| Приложение 1. Название приложения........................................................ |  | 60 |
| Приложение 2. Название приложения........................................................ |  | 61 |

ПРИЛОЖЕНИЕ 4. оПРЕДЕЛЕНИЯ, ОБОЗНАЧЕНИЯ, СОКРАЩЕНИЯ

Определения, обозначения и сокращения

|  |  |
| --- | --- |
| СОА | Система обнаружения атак |
| КИИ | Критическая информационная инфраструктура |
| ГосСОПКА | Государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |