ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

**Московский институт электроники и математики им. А.Н. Тихонова**

Фамилия Имя Отчество автора

**НАЗВАНИЕ ТЕМЫ ВКР**

Выпускная квалификационная работа – магистерская диссертация

по направлению 10.04.01 «Информационная безопасность»

студента образовательной программы магистратуры  
«Наименование образовательной программы»

|  |  |
| --- | --- |
| Студент  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  И.О. Фамилия  Рецензент  уч. степень, уч. звание  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  И.О. Фамилия | Научный руководитель  уч. степень, уч. звание  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  И.О. Фамилия  Консультант  уч. степень, уч. звание  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  И.О. Фамилия |

Москва 2025

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ АВТОНОМНОЕ

ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ УНИВЕРСИТЕТ

«ВЫСШАЯ ШКОЛА ЭКОНОМИКИ»

**Московский институт электроники и математики им. А.Н. Тихонова**

**ЗАДАНИЕ**

**на выполнение выпускной квалификационной работы**

студенту группы \_\_\_\_\_ Фамилия Имя Отчество

1. Тема работы

*Тема ВКР приводится в соответствии с приказом об утверждении тем ВКР.*

1. Требования к работе

2.1. Цель работы

*Цель работы формулируется в контексте повышения эффективности некоторого научно-технического решения либо в контексте решения конкретной прикладной задачи. Из формулировки цели ВКР должна быть понятна ее актуальность*.

2.2. Требования к результатам работы

*Перечисляются основные результаты, которые должны быть получены в рамках ВКР, и уточняются их технические характеристики.*

2.3. Требования к документации

Текст ВКР должен быть оформлен в соответствии с ГОСТ.

1. Содержание работы

*Перечисляются основные выполняемые работы, в основном соответствующие структуре ВКР, представленной в пояснительной записке. Обязательные работы приведены в настоящем шаблоне. Все прочие работы определяются студентом совместно с руководителем.*

3.1. Обзор научно-технической литературы по теме работы

3.2. …

3.\_. Подготовка пояснительной записки к ВКР

1. Сроки выполнения этапов работы

|  |  |
| --- | --- |
| Проект ВКР представляется студентом в срок до | «16» февраля 2025 г. |
| Первый вариант ВКР представляется студентом в срок до | «31» марта 2025 г. |
| Итоговый вариант ВКР представляется студентом руководителю до загрузки работы в систему «Антиплагиат» в срок до | «30» апреля 2025 г. |

|  |  |  |
| --- | --- | --- |
| Задание выдано | «20» декабря 2024 г. | \_\_\_\_\_\_\_\_\_\_\_\_ И.О. Фамилия  подпись руководителя |
|  |  |  |
| Задание принято к исполнению | «20» декабря 2024 г. | \_\_\_\_\_\_\_\_\_\_\_\_ И.О. Фамилия  подпись студента |

**Аннотация**

В аннотации кратко описывается решаемая в выпускной квалификационной работе (ВКР) задача, обосновывается ее актуальность, описываются использованные методы и приводятся полученные результаты. При описании полученных результатов указываются их отличительные особенности и преимущества. Работа содержит \_\_ страниц, \_\_ рисунков, \_\_ таблиц, \_\_ источников, \_\_ приложений.

**Abstract**

Перевод аннотации на английский язык.

**СОДЕРЖАНИЕ**

[1 Введение 7](#__RefHeading___Toc3438_1511805350)

[2 Обзор литературы 8](#__RefHeading___Toc3440_1511805350)

[2.1 SCA для Java-проектов с использованием Spring Boot 8](#__RefHeading___Toc3442_1511805350)

[2.1.1 SCA opensource иностранные 10](#__RefHeading___Toc3444_1511805350)

[2.1.2 SCA отечественные 10](#__RefHeading___Toc3446_1511805350)

[2.2 Название подраздела 10](#__RefHeading___Toc3448_1511805350)

[2.2.1 Название пункта 10](#__RefHeading___Toc3450_1511805350)

[2.2.2 Название пункта 10](#__RefHeading___Toc3452_1511805350)

[3 Заключение 11](#__RefHeading___Toc3454_1511805350)

[4 Список использованных источников 12](#__RefHeading___Toc3456_1511805350)

[ПРИЛОЖЕНИЕ А. Основные требования к оформлению текста ВКР 13](#__RefHeading___Toc3458_1511805350)

[ПРИЛОЖЕНИЕ Б. Пример списка использованных источников 19](#__RefHeading___Toc3460_1511805350)

# 1 Введение

Цель данной работы заключается в повышении эффективности разработки и обеспечения безопасности микросервисов, построенных на платформе Java Spring Boot, путем интеграции методов статического и динамического анализа, а также анализа состава программного обеспечения. В частности, акцент будет сделан на использовании инструментов SCA (Software Composition Analysis), SAST (Static Application Security Testing) и DAST (Dynamic Application Security Testing).

В рамках исследования будет изучено применение опенсорсных библиотек, доступных для скачивания в России, что обеспечит доступность и возможность практической реализации предложенных решений. Особое внимание будет уделено поиску и оценке русских аналогов анализируемых инструментов, если таковые найдутся.

В результате работы будет представлена практическая реализация интеграции инструментов SCA и SAST в процесс разработки микросервисов, что позволит продемонстрировать их взаимодополняемость и вклад в повышение уровня безопасности приложений. Кроме того, будет рассмотрено применение DAST в рамках тестирования и эксплуатации, что подчеркнет важность комплексного подхода к обеспечению безопасности. Таким образом, работа направлена не только на решение конкретных прикладных задач, но и на развитие понимания актуальных методов обеспечения безопасности в контексте современного программного обеспечения.

# 2 Обзор литературы

В этой главе я проведу обзор литературы, посвященной инструментам статического и динамического анализа программного обеспечения (SCA, SAST и DAST), с акцентом на их применение в контексте разработки Java-приложений, использующих библиотеку Spring Boot.

Также я буду рассматривать использование этих инструментов в процессах непрерывной интеграции и доставки (CI/CD), что является важной частью практик DevSecOps. Одним из ключевых аспектов внедрения SAST и DAST инструментов должно быть их удобство интеграции в существующие рабочие процессы разработки. Эти инструменты должны быть легко подключяемы к CI/CD конвейерам.

## 2.1 ****SCA для Java-проектов с использованием Spring Boot****

Компоненты с открытым исходным кодом стали основными элементами программного обеспечения в различных областях. Системы SCA помогают контролировать эти компоненты в приложениях, что критично для их безопасности. Всё больше современных приложений строится на базе открытого кода, и по некоторым данным, до 90% их кода может состоять из опенсорса [1]. Анализ компонентов программного обеспечения (SCA) представляет собой процесс идентификации и оценки компонентов, особенно открытого исходного кода, в рамках программного обеспечения, а также проверки их безопасности. Используя SCA, команды разработчиков могут быстро обнаруживать и анализировать опенсорсные компоненты, интегрированные в проект. Инструменты SCA способны выявлять все связанные компоненты и библиотеки, а также прямые и косвенные зависимости. Кроме этого, системы SCA выявляют лицензии программного обеспечения, устаревшие зависимости, уязвимости и потенциальные угрозы.

В результате сканирования создаётся полная спецификация, которая позволяет провести инвентаризацию программных активов проекта. Хотя инструменты SCA существуют уже давно, их значение возросло с увеличением использования открытого исходного кода в последние годы, и они стали ключевыми для повышения безопасности приложений. Современные методологии разработки, такие как DevSecOps, требуют, чтобы SCA был удобен как для разработчиков, так и для специалистов по безопасности, чья роль заключается в поддержке разработчиков на всех этапах жизненного цикла разработки программного обеспечения.

В области разработки программного обеспечения эффективное управление зависимостями является ключевым аспектом в создании надежных и безопасных приложений. Spring Boot, который зарекомендовал себя как предпочтительный инструмент среди разработчиков на языке Java, значительно упрощает процесс разработки, однако не следует ограничиваться лишь его удобством. Критически важно осуществлять мониторинг и актуализацию зависимостей, чтобы обеспечить бесперебойную работу проектов на Spring Boot и их устойчивость к постоянно эволюционирующим угрозам [2].

Одним из наиболее важных аспектов управления зависимостями в рамках Spring Boot является вопрос безопасности. Уязвимости в программном обеспечении регулярно выявляются, и своевременное обновление зависимостей в проекте можно рассматривать как форму цифровой защиты. Устаревшие зависимости представляют собой потенциальные риски, аналогичные незапертым дверям, которые могут способствовать проникновению угроз. Следовательно, необходимо принять меры для предотвращения таких ситуаций и обеспечить безопасность и целостность разрабатываемых приложений [2].

Gradle и Maven — это популярные инструменты для управления проектами и построения программного обеспечения на языке Java. Они упрощают процесс сборки, управления зависимостями и автоматизации рабочего процесса, позволяя разработчикам сосредоточиться на написании кода, а не на решении организационных задач.

В ходе обзора средств анализа компонентов программного обеспечения (SCA) для Java-приложений я отметила, что фреймворки SCA различаются по удобству использования для разработчиков. К менее удобным инструментам можно отнести те, которые требуют локальной установки для анализа кода, что подразумевает необходимость запуска исполняемого файла приложения. В то же время существуют более удобные SCA-инструменты, которые позволяют легко добавлять зависимости в Gradle или Maven, после чего их можно использовать непосредственно через эти системы управления проектами.

В следующей части работы будет представлен обзор международных опенсорсных SCA-инструментов, которые я бы захотела использовать благодаря их удобству и эффективности. Также мне удалось обнаружить перспективный отечественный SCA-инструмент, о котором стоит рассказать.

### 2.1.1 **Обзор иностранных опенсорсных SCA-инструментов**

Текст.

### 2.1.2 **Обзор отечественных SCA-инструментов**

Текст.

## 2.2 Название подраздела

Текст.

### 2.2.1 Название пункта

Текст.

### 2.2.2 Название пункта

Текст.

# 3 Заключение

Приводится краткое описание результатов ВКР.

# 4 Список использованных источников

1. Обзор рынка инструментов SCA (Software Composition Analysis) – URL: https://www.anti-malware.ru/analytics/Market\_Analysis/Software-Composition-Analysis (дата обращения 15.01.2025).

2. Handling security vulnerabilities in Spring Boot | Snyk. – URL: https://snyk.io/blog/security-vulnerabilities-spring-boot/ (дата обращения 15.01.2025).

# ПРИЛОЖЕНИЕ А. Основные требования к оформлению текста ВКР

**А.1 Общие требования к оформлению текста ВКР**

Шрифт: единый, рекомендуемый – Times New Roman,

Цвет: черный,

Размер: не менее 12 пт., одинаковый во всем документе,

Выравнивание текста – по ширине,

Межстрочный интервал – полуторный (исключения: оформление титула, названий рисунков и таблиц),

Абзацный отступ – 1,25 см.,

Отступы и интервалы в тексте – 0 см.

Полужирный шрифт**:** применяют только для заголовков структурных элементов документа,для заголовков разделов и подразделов основной части документа.

Курсив:допускается для обозначения объектов и написания терминов. Курсив также может использоваться для *акцентирования внимания, выделения текста в документе*, но при этом текст должен быть *того же кегля и гарнитуры*. Разрешается для написания определенных терминов, формул, теорем применять шрифты разной гарнитуры.

Размеры полей:левое – 3,0 см., правое – 1,5 см., верхнее и нижнее – 2,0 см.

Номера страниц– арабскими цифрами, *внизу по центру***.** Титульный листвключают в общую нумерацию страниц документа. *Номер* страницы на титульном листе *не проставляют*. *Приложения* должны иметь общую с остальной частью документа сквозную нумерацию страниц.

Оформление перечислений**:** перед каждым элементом перечисления следует ставить *тире* или, при необходимости ссылки в тексте документа на один из элементов перечисления, вместо тире ставят *строчные буквы,* начиная с буквы «а» (за исключением – е, з, й, о, ч, ъ, ы, ь), после которой ставится скобка. Простые перечисления отделяются запятой, сложные – точкой с запятой.

*НЕ*допускается использование *данных**знаков*:



При наличии конкретного числа перечислений допускается использовать *арабские цифры* со скобками.

Перечисления приводятся с абзацного отступа – 1,25 пт., без отступов слева и выступов справа.

**А.2 Оформление иллюстраций**

К иллюстрациям относятся: чертежи, графики, схемы, диаграммы, фотоснимки.

Иллюстрации следует располагать *непосредственно после текста*, где они упоминаются впервые, или на следующей странице (по возможности ближе к соответствующим частям текста).

На все иллюстрации в тексте документа должны быть даны ссылки. При ссылке необходимо писать слово «рисунок» и его номер, например: «в соответствии с рисунком 2». *Не допускается*сокращение типа *Рис.5.*

Иллюстрации, за исключением иллюстраций, приведенных в приложениях, следует нумеровать арабскими цифрами сквозной нумерацией: Рисунок 1.

Допускается нумеровать иллюстрации в пределах раздела документа. В этом случае номер иллюстрации состоит из номера раздела и порядкового номера иллюстрации, разделенных точкой: Рисунок 1.1.

Если рисунок в документе всего один, то он обозначатся: Рисунок 1.

Иллюстрации должны иметь наименование и пояснительные данные (подрисуночный текст). Слово «Рисунок», его номер и через тире наименование помещают после пояснительных данных и располагают в центре под рисунком.

Пример оформления названия рисунка:

Рисунок 1.1 – Если наименование рисунка состоит из нескольких строк, то его записывают через один межстрочный интервал. Наименование рисунка приводят с прописной буквы без точки в конце. Перенос слов в наименовании рисунка не допускается

**А.3 Оформление таблиц**

Таблицу следует располагать непосредственно после текста, в котором она упоминается впервые, или на следующей странице.

На все таблицы документе должны быть ссылки. При ссылке следует печатать слово «таблица» с указанием ее номера***.*** *Не допускается сокращение – Табл*.5.

Допускается применять размер шрифта в таблице меньший, чем в основном тексте документа.

Таблицы, за исключением таблиц приложений, следует нумеровать арабскими цифрами сквозной нумерацией.

Допускается нумеровать таблицы в пределах раздела при большом объеме документа. В этом случае номер таблицы состоит из номера раздела и порядкового номера таблицы, разделенных точкой: Таблица 2.3.

Наименование таблицы следует помещать над таблицей слева без абзацного отступа в одну строку с ее номером через тире, например,Таблица 1 – Наименование. Наименование таблицы приводят с прописной буквы без точки в конце. Если наименование таблицы занимает две строки и более, то его следует записывать через *один межстрочный интервал*.

Если таблица занимает больше двух страниц, то при переносе части таблицы на другую страницу пишут слова «Продолжение таблицы 1», пример оформления названия таблицы:

Таблица 1.1 – Наименование таблицы следует помещать над таблицей слева без абзацного отступа с прописной буквы в одну строку с ее номером через тире без точки в конце. Если наименование таблицы занимает две строки и более, то его следует записывать через один межстрочный интервал

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Продолжение таблицы 1.1

|  |  |  |  |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**А.4 Оформление формул и уравнений**

Уравнения и формулы следует выделять из текста в отдельную строку. Выше и ниже каждой формулы или уравнения должно быть оставлено *не менее одной свободной строки*. Если уравнение не умещается в одну строку, оно должно быть перенесено после знака равенства (=) или после знаков плюс (+), минус (–), умножения (×), деления (:) или других математических знаков. На новой строке знак повторяется.

Пояснение значений символов и числовых коэффициентов следует приводить непосредственно под формулой в той же последовательности, в которой они представлены в формуле. Значение каждого символа и числового коэффициента необходимо приводить с новой строки. Первую строку пояснения начинают со слова «где» без двоеточия с абзаца.

Формулы следует располагать *посередине строки* и обозначать порядковой нумерацией в пределах всего документа арабскими цифрами в круглых скобках в крайнем правом положении на строке. Одну формулу обозначают (1).

Ссылки на порядковые номера формул приводятся в скобках в формуле (1).

Допускается нумерация формул в пределах раздела. В этом случае номер формулы состоит из номера раздела и порядкового номера формулы, разделенных точкой: (3.1)

Пример:

Для рядов данных *x, y* коэффициенты линейных зависимостей *a, b (y*=*a*+*bx)* рассчитываются, как решение системы уравнений (3.1):

|  |  |
| --- | --- |
| , | (3.1) |

где *x* – средние или максимальные значения температуры процессоров;

*y* – температуры на выходе бака;

, – среднее арифметическое значение элементов ряда.

**А.5 Оформление списка использованных источников**

Список должен содержать сведения об источниках, использованных при составлении документа. Сведения об источниках приводятся в соответствии с требованиями ГОСТ 7.1, [ГОСТ 7.80](consultantplus://offline/ref=1664E79CF97BFD0858C3BB176F68BD1AE7E0C40EC8784F205FE14ABC80BBR0M), [ГОСТ 7.82](consultantplus://offline/ref=1664E79CF97BFD0858C3AD1B6D68BD1AEAEBC600CA2A18220EB444BBR9M) (пример приведен в Приложении Б).

Сведения об источниках следует располагать в порядке появления ссылок на источники в тексте документа и нумеровать арабскими цифрами с точкой и печатать с абзацного отступа.

Список использованных источников должен включать библиографические записи на документы, использованные при составлении документа, ссылки на которые оформляют арабскими цифрами в квадратных скобках [1], [3]–[10] в тексте документа. На каждый источник в тексте документа должна быть такая ссылка.

# ПРИЛОЖЕНИЕ Б. Пример списка использованных источников

1. DeRidder J.L. The immediate prospects for the application of ontologies in digital libraries// Knowledge Organization – 2007 . – Vol. 34, No. 4 . – P. 227 – 246 .

2. Прогноз научно-технологического развития Российской Федерации на период до 2030 года . – URL: http://government.ru/media/files/41d4b737638891da2184/pdf (дата обращения 15.11.2016).

15.11.2016).

12. Леготин Е.Ю. Организация метаданных в хранилище данных// Научный поиск. Технические науки: Материалы 3-й науч. конф. аспирантов и докторантов/отв. за вып. С.Д. Ваулин; Юж.-Урал. гос. ун-т. Т. 2. – Челябинск: Издательский центр ЮУрГУ , 2011 – С. 128 – 132 .

13. Статистические показатели российского книгоиздания в 2006 г.: цифры и рейтинги [Электронный ресурс]. – 2006. – URL: http://bookhamber.ru/stat\_2006.htm (дата обращения 12.03.2009).

14. Приказ Минобразования РФ от 19 декабря 2013 г. N 1367 «Об утверждении Порядка организации и осуществления образовательной деятельности по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры». – URL: http://www. consultant.ru/document/cons\_doc\_LAW\_159671 (дата обращения 04.08.2016).

15. ГОСТ 7.0.96-2016 Система стандартов по информации, библиотечному и издательскому делу. Электронные библиотеки. Основные виды. Структура. Технология формирования. – М: Стандартинформ, 2016 . – 16 с.