

МИНОБРНАУКИ РОССИИ

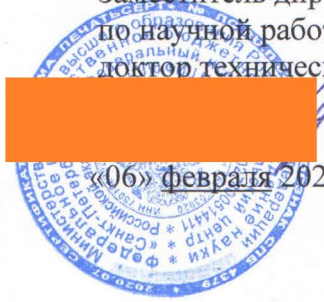
**Федеральное государственное  
бюджетное учреждение науки  
«Санкт-Петербургский  
Федеральный исследовательский центр  
Российской академии наук»  
(СПб ФИЦ РАН)**

14-я линия, д. 39, г. Санкт-Петербург, 199178  
Тел.: (812) 328-33-11, факс: (812) 328-44-50,  
e-mail: info@spcras.ru, web: http://www.spcras.ru  
ОКПО 04683303, ОГРН 1027800514411,  
ИНН/КПП 7801003920/780101001

«06» февраля 2024 № 60/01-01-90

УТВЕРЖДАЮ

Заместитель директора СПб ФИЦ РАН  
по научной работе  
доктор технических наук



Кулешов С.В.

«06» февраля 2024 года

## ОТЗЫВ ВЕДУЩЕЙ ОРГАНИЗАЦИИ

на диссертацию Шарикова Павла Ивановича,  
выполненную на тему

**«Разработка стратифицированных методик создания и вложения устойчивого к  
атакам декомпиляцией и обфускацией цифрового водяного знака в байт-код class-  
файлов java-приложений и информационных систем»,**

представленной на соискание ученой степени кандидата технических наук по  
специальности 2.3.6 – «Методы и системы защиты информации, информационная  
безопасность»

### 1. Актуальность темы диссертационной работы

Язык программирования Java является, как известно, одним из самых распространенных языков в мире. Появляются новые языки программирования, но на текущий момент чаще всего для разработки сложных информационных государственных, банковских систем используется язык Java. С каждым годом количество информационных систем увеличивается, а это означает, что потенциальные кражи исходного кода злоумышленниками также возрастают. Таким образом, актуальность защиты java-приложений и информационных систем как интеллектуальной собственности с каждым годом только растет.

Цифровые водяные знаки в исполняемых файлах, позволяющие доказать авторство на исходный код java-приложения или информационной системы, могут решить эту проблему. Существующие методики вложения цифровых водяных знаков в исполняемые

class-файлы являются не актуальными на текущий момент. Цифровые водяные знаки, вложенные в class-файлы данными методиками, легко удаляются атаками и легко обнаруживаются, так как занимают малый объем в class-файле.

Исходя из всего вышеперечисленного, следует констатировать, что тема и результаты диссертационной работы Шарикова Павла Ивановича, посвященные повышению объема цифрового водяного знака и его устойчивости к атакам, являются достаточно **актуальными**.

Результаты анализа проблематики исследуемой предметной области предопределили **объект исследования** – байт-код исполняемых файлов Java и **предмет исследования**, который составили методики создания и вложения устойчивого к атакам цифрового водяного знака в байт-коде class-файлов.

Целью работы является повышение объема цифрового водяного знака и его устойчивости к атакам за счет эквивалентных замен операционных кодов байт-кода Java-приложения.

**Научная задача**, решаемая в диссертационной работе, определена автором как разработка методик создания и вложения увеличенного объема и устойчивого к атакам цифрового водяного знака в байт-коде class-файлов java-приложений и информационных систем.

## **2. Новизна исследования и полученных результатов выводов и рекомендаций, сформулированных в диссертации**

С учетом постоянного развития, обновления и модернизации информационных систем, языков программирования и их экосистем, исследования и существующие методики устаревают, теряют актуальность, становятся неприменимыми на новых версиях языка программирования или виртуальных машинах для интерпретируемых языков программирования.

Диссертационная работа Шарикова Павла Ивановича обладает отличительными признаками новизны. Автором используются расширенный набор операционных кодов (опкодов) виртуальной машины Java, по сравнению с ранними работами на данную тему. Методики позволяют произвести вложение цифрового водяного знака, который является неотъемлемой частью class-файла. Повышен объем цифрового водяного знака в class-файле, используются методы и конструкции, затрудняющие декомпиляцию class-файлов, а также анализ взаимосвязей модулей информационной системы, результаты которого используются при создании цифрового водяного знака регистратора.

**Научная новизна** работы заключается в том, что в ней, в отличие от известных, предложены методики, позволяющие произвести создание и скрытое вложение цифрового водяного знака в байт-код class-файлов java-приложений и информационных систем. Предложенные методики позволяют:

- произвести вложение цифрового водяного знака большего объема за счет использования расширенного набора опкодов для эквивалентных замен, использования в качестве контейнера всего class-файла с доступными опкодами, не ограничиваясь фиктивными методами;
- произвести вложение цифрового водяного знака, устойчивого к атакам перекомпиляции, за счет использования функций, затрудняющих декомпиляцию;
- произвести вложение двух видов цифровых водяных знаков в java-приложения информационной системы на основе анализа взаимосвязей ключевых модулей информационной системы.

Научная новизна исследования подтверждается результатами практических экспериментов на реальных объектах, актами о внедрении, публикациями в журналах из перечня ВАК, зарубежных журналах из перечня Scopus, объектами интеллектуальной собственности.

### **3. Обоснованность и достоверность научных положений и выводов**

Из содержания разделов диссертационной работы следует, что основные научные результаты, выносимые на защиту, сформулированы **обоснованно**, обладают научной новизной и отражают оригинальность решений. К ним следует отнести:

1. Методику создания и скрытого вложения цифрового водяного знака в байт-код class-файла на основе недеklarированных возможностей виртуальной машины Java.
2. Методику создания и вложения цифрового водяного знака в class-файлы java-приложения, устойчивого к атакам декомпиляцией, направленным на его разрушение.
3. Методику создания и вложения цифрового водяного знака в class-файлы информационной системы, устойчивого к атакам обфускацией, направленным на его разрушение.

**Достоверность** основных выводов и результатов диссертации подтверждается:

- всесторонним анализом предшествующих научных работ в области вложения цифровых водяных знаков в исполняемые файлы, принципов работы новейших версий языка программирования и виртуальной машины Java, принципов взаимодействия различных опкодов с виртуальной машиной Java, документации к виртуальной машине

Java и механизмов выбора операционных кодов для различных действий в логике исходного кода;

- корректностью постановки научной задачи;
- обоснованием выбора контейнера для цифрового водяного знака, исследованием функций, затрудняющих работу существующих декомпиляторов, экспериментальной проверкой разработанных методик, оценке эффективности методик посредством метрик исходного кода и поведения java-приложений;
- применением полученных результатов в тематических НИР, а также полученными реализациями и апробациями.

#### **4. Значимость для науки и практики результатов, полученных автором диссертации**

**Теоретическая значимость** полученных результатов исследования обусловлена их научной новизной и заключается в том, что:

сделан вклад в развитие теории методик создания и вложения цифрового водяного знака в исполняемые файлы, заключающийся в доказательстве возможности использования расширенного набора операционных команд байт-кода для создания и вложения цифрового водяного знака в class-файлы посредством эквивалентных замен;

доказана возможность вложения устойчивого к атакам декомпиляцией цифрового водяного знака в class-файлы java-приложения и доказана устойчивость цифрового водяного знака к атакам декомпиляцией;

доказана возможность вложения устойчивого к атакам обфускацией цифрового водяного знака в class-файлы информационной системы.

**Практическая значимость** работы заключается в том, что полученные результаты могут быть использованы:

1. Для создания и скрытого вложения цифрового водяного знака в байт-код class-файла с использованием расширенного набора операционных команд виртуальной машины Java;

2. Для создания и вложения цифрового водяного знака в class-файлы java-приложения, устойчивого к атакам декомпиляцией, направленным на его разрушение;

3. Для создания и вложения цифрового водяного знака в class-файлы информационной системы, устойчивого к атакам обфускацией, направленным на его разрушение.

Кроме того, практическая значимость работы определяется доведением полученных в ней решений до уровня программной реализации, что подтверждается наличием трех зарегистрированных программ для ЭВМ.

## 5. Рекомендации по использованию результатов и выводов диссертации

Разработанные методики:

- создания и скрытого вложения цифрового водяного знака в байт-код class-файла на основе недекларированных возможностей виртуальной машины Java;
- создания и вложения цифрового водяного знака в class-файлы java-приложения, устойчивого к атакам декомпиляцией, направленным на его разрушение;
- создания и вложения цифрового водяного знака в class-файлы информационной системы, устойчивого к атакам обфускацией, направленным на его разрушение

были использованы в мероприятиях по выработке перспективных подходов для вложения цифрового водяного знака в исполняемые файлы программного обеспечения, предназначенного для тестирования телекоммуникационного оборудования в ООО «ДИЛЕР» и в учебном процессе СПбГУТ, о чем свидетельствуют полученные акты внедрения. Разработаны программы для ЭВМ «Модификатор байт-кода java-программы для скрытого вложения цифрового водяного знака посредством автоматического редактирования байт-кода class-файла», «Анализатор байт-кода java-программы для скрытого вложения цифрового водяного знака посредством автоматического редактирования байт-кода class-файла» и «Программное обеспечение по реализации стеганографических методов при передаче сообщения», на которые получены свидетельства о государственной регистрации.

Дальнейшие исследования и внедрение рекомендуется проводить в организациях, использующих сложные высоконагруженные информационные системы, составляющие коммерческую тайну, банковскую тайну и органах исполнительной власти, эксплуатирующих государственные информационные системы, а также в учебном процессе в ВУЗах.

## 6. Общая оценка диссертационной работы

Анализ диссертации показал, что её структура характеризуется внутренним единством и логической связанностью. Диссертация состоит из содержания, введения, 4 глав, заключения, списка сокращений, списка литературы и приложений. По своему содержанию диссертация **соответствует паспорту искомой специальности** — «Методы и системы защиты информации, информационная безопасность», по оформлению — соответствует требованиям, предъявляемым к научным работам, направляемым в печать.

Во введении приводится обоснование актуальности темы диссертационного исследования, определяются цели и задачи исследования, предмет и объекты исследования. Обоснованы новизна и практическая ценность результатов, выносимых на защиту. Дана краткая характеристика содержания работы, приведены сведения о

внедрении результатов диссертационного исследования, сведения об апробации результатов работы.

В первой главе приведены результаты анализа существующих работ по тематике диссертационной работы, сделаны выводы о их актуальности и практической применимости на текущий момент.

Во второй главе представлена методика создания и вложения цифрового водяного знака в class-файле на основе эквивалентных замен опкодов, расширенного набора.

В третьей главе представлена методика создания и вложения цифрового водяного знака в class-файлы java-приложения. Учитывается анализ взаимосвязей class-файлов внутри одного java-приложения, а также используются функции, затрудняющие декомпиляцию и повторную компиляцию class-файлов.

В четвертой главе представлена методика создания и скрытого вложения цифрового водяного знака регистратора, устойчивого к атакам обфускацией, в байт-код class-файлов java-приложений информационной системы. В данной методике анализируются связи между ключевыми модулями информационной системы с последующим использованием полученной информации при создании цифрового водяного знака регистратора. Также производится создание и вложение цифрового водяного знака в ключевые class-файлы каждого java-приложения информационной системы.

#### **Замечания по диссертационной работе:**

1. Не в полной мере обоснован выбор операционных кодов расширенного набора для эквивалентных замен.
2. Недостаточно обоснован выбор статического редактирования байт-кода с целью вложения цифрового водяного знака в class-файлы.
3. Не в полной мере обоснована неэффективность использования «мертвого кода» и фиктивных методов в исходном коде для вложения цифрового водяного знака.
4. В диссертационной работе указывается, что верификатор виртуальной машины Java может пометить class-файл как поврежденный и не дать разрешения на его исполнение в виртуальной машине Java при не прохождении одной из его проверок. Однако не раскрыто, как эквивалентные замены, производимые в class-файле, могут быть интерпретированы верификатором, и какие существуют риски.
5. Не в полной мере раскрыто влияние эквивалентных замен на объем class-файла.

Перечисленные замечания не влияют на полученные в работе результаты, ее теоретическую и практическую значимость. Поставленные задачи в работе выполнены в полном объеме, цель исследования достигнута.

## 7. Заключение

Диссертация Шарикова Павла Ивановича на тему «Разработка стратифицированных методик создания и вложения устойчивого к атакам декомпиляцией и обфускацией цифрового водяного знака в байт-код class-файлов java-приложений и информационных систем» является законченной научно-квалификационной работой, в которой содержится решение задачи разработки методик создания и вложения цифрового водяного знака в байт-код class-файлов java-приложений и информационных систем увеличенного объема и устойчивого к атакам. Цель работы, поставленные и выполненные в ней задачи являются актуальными. Полученные результаты и положения, выдвигаемые автором на публичную защиту, имеют научную новизну, теоретическую и практическую значимость. Диссертация выполнена единолично, имеет внутреннее единство. Результаты работы свидетельствуют о личном вкладе автора в науку.

Работа соответствует критериям, предъявляемым в отношении кандидатских/докторских диссертаций, которые установлены пп. 9–14 Положения о присуждении ученых степеней (утв. Постановлением Правительства РФ от 24.09.2013 № 842), а ее автор Шариков Павел Иванович заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность».

Диссертация и автореферат заслушаны и обсуждены на научном семинаре лаборатории проблем компьютерной безопасности 06 февраля 2024 года, протокол № 4.

Главный научный сотрудник лаборатории проблем компьютерной безопасности Федерального государственного бюджетного учреждения науки «Санкт-Петербургского Федерального исследовательского центра Российской академии наук», доктор технических наук, профессор

  
Саенко Игорь Борисович

Старший научный сотрудник лаборатории проблем компьютерной безопасности Федерального государственного бюджетного учреждения науки «Санкт-Петербургского Федерального исследовательского центра Российской академии наук», кандидат технических наук, доцент

  
Новикова Евгения Сергеевна