ОТЗЫВ

на автореферат **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», по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность

Актуальность диссертационной работы.

Информационные системы все чаще используются. С помощью информационных систем осуществляется обработка различного рода информации в организациях и предприятиях из разных сфер деятельности. Начиная от учебных организаций заканчивая оборонными. Многие из систем разрабатываются на языке программирования Java, так как данный язык хорошо зарекомендовал себя для решения серверных задач. Однако у данного языка существуют недостатки, одним из которых является легкость получения исходного кода из исполняемых файлов. Следовательно, такие информационные системы и исполняемые файлы в них, необходимо каким-либо образом отслеживать, если происходит компрометация.

Защита исходного кода Java и исполняемых class-файлов цифровыми водяными знаками (ЦВЗ) имеет несколько целей и преимуществ: аутентификация и подлинность; защита интеллектуальной собственности; обнаружение и предотвращение подделок исполняемых файлов; улучшение контроля над лицензированием и распространением. Однако в следствии того, что язык программирования, его экосистема, подходы к разработке информационных систем постоянно изменяются и совершенствуются, существующие методики устаревают, необходима разработка новых более эффективных, направленных на работу с существующими и активно эксплуатируемыми java-приложениями информационными системами.

Таким образом, исходя из описанных выше актуальных проблем, диссертационная работа 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 актуальной.

Положения, выносимые на защиту

1. Методика создания и скрытого вложения цифрового водяного знака в байт-код class-файла на основе не декларированных возможностей виртуальной машины Java.

2. Методика создания и вложения цифрового водяного знака в class-файлы java-приложения устойчивого к атакам декомпиляцией направленных на его разрушение.

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

Теоретическая значимость работы

1. Показано, что использование расширенного набора операционных команд для создания и вложения цифрового водяного знака в class-файлы посредством эквивалентных замен допустимо и не несет в себе рисков для работоспособности исполняемого файла

2. Установлена возможность вложения цифрового водяного знака в исполняемые файлы java-приложения, который является устойчивым к атакам декомпиляцией. Исследована устойчивость цифрового водяного знака к атакам декомпиляцией.

3. Исследована устойчивость цифрового водяного знака к атакам обфускацией. Установлен высокий риск приведения исполняемого файла, java-приложения или информационной системы в неработоспособное состояние посредством применения инструментов продвинутой обфускации.

Практическая значимость работы

Предложенные методики могут быть использованы при разработке программных средств для анализа и защиты программных систем. Такие программные средства будут обеспечивать возможность вложить цифровой водяной знак большего объема по сравнению с существующими методиками, повысить устойчивость к атакам декомпиляцией за счет шаблонов и паттернов проектирования слабо поддающихся анализу через байт-код и дальнейшей обратной интерпретации в исходный код программы и устойчивость к атакам обфускацией за счет анализа взаимосвязей модулей информационной системы и вложения цифрового водяного знака в каждый модуль информационной системы.

Научная новизна работы заключается в особенностях предложенных методик, позволяющих затруднить декомпиляцию и уничтожение или разрушения цифрового водяного знака, в частности, за счет использования расширенного набора опкодов и анализа связанности модулей информационной системы с целью создания цифрового водяного знака регистратора, охватывающего все модули информационной системы.

Обоснованность и достоверность результатов, выносимых на защиту диссертационного исследования, выводов научного характера

подтверждаются математическим обоснованием результатов исследований, системным подходом к решению поставленных задач, обоснованием выбранных показателей оценки эффективности предложенных методик, доказательствами и результатами экспериментальной проверки предложенных методик, анализом существующих зарубежных и отечественных работ данной тематики, апробацией результатов на международных и российских конференциях, а также подтверждением о внедрении предложенных методик в организациях и предприятиях.

Результаты, выносимые на защиту, соответствуют пунктам 7, 17 паспорта научной специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Замечания к автореферату:

- В работе отсутствует формальное описание методов внедрения и извлечения ЦВЗ. Раздел с описанием примера создания и вложения ЦВЗ в class-файл позволяет косвенно выделить некоторые особенности предлагаемого метода, но явно недостаточен при отсутствии формального описания. Про извлечение не сказано практически ничего. Более того, из текста работы не ясно, к какому типу методов маркирования относится метод - zero-bit (декодер определяет факт присутствия метки в контейнере) или multi-bit (декодер выдает битовую последовательность определенной длины).
- В работе мало внимания уделяется вопросу извлечения ЦВЗ, хотя указывается на то, что наличие способа извлечения является характеристикой эффективности того или иного вида ЦВЗ.
- Практически не раскрыт вопрос программной реализации. Автор описывает методики и алгоритмы, которые формализуют эти методики. При этом структура и методы построения программного решения не рассматриваются. Кроме того, сравнительный анализ известных и новых алгоритмов проводится лишь на тестовых примерах, а хотелось бы увидеть данные, полученные на образцах промышленного ПО.

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

Заключение.

Диссертация Шарикова П.И. 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. Цель работы является актуальной. Положения, выдвигаемые автором на публичную защиту, имеют научную новизну, теоретическую и практическую значимости.

Диссертационная работа удовлетворяют требованиям ВАК при Минобрнауки России и пунктам 9 – 14 «Положения о присуждении ученых степеней», утвержденным постановлением Правительства Российской Федерации от 24.09.2013 г. № 842, предъявляемым к кандидатским диссертациям, а соискатель Шариков Павел Иванович заслуживает присуждения ему ученой степени кандидата технических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

Отзыв составил:

Заведующий отделом Технологий программирования,
доктор физико-математических наук, профессор

[redacted] Александр Константинович Петренко

15 февраля 2024 года

Подпись А.К. Петренко заверяю

Ученый секретарь Федерального государственного бюджетного учреждения науки Институт системного программирования им. В. П. Иванникова Российской Академии Наук,
канд. тех. наук [redacted] /О. И. Самоваров/

15 февраля 2024 года

Почтовый адрес: 109004, г. Москва, ул. Александра Солженицына, д. 25.

Тел.: 8 (495) 912-44-25.

e-mail: info-isp@ispras.ru