«УТВЕРЖДАЮ»
Директор Федерального
государственного учреждения
«Федеральный исследовательский
центр «Информатика и управление»
Российской академии наук»,
~~Член~~-корреспондент РАН

М.А. Посыпкин

«29» ноября 2024 г.

ОТЗЫВ

ведущей организации – Федерального государственного учреждения «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» – на диссертацию Обыденкова Дмитрия Олеговича «Методы противодействия анонимности при утечках текстовых документов посредством цифровых водяных знаков», представленную на соискание ученой степени кандидата технических наук по специальности 2.3.5 – Математическое и программное обеспечение вычислительных систем, комплексов и компьютерных сетей

Диссертационная работа Д.О. Обыденкова посвящена исследованию и разработке методов противодействия анонимности при утечках текстовых документов посредством цифровых водяных знаков (ЦВЗ). Предложенные в работе подходы направлены на предотвращение несанкционированной передачи документов, оцифрованных после печати или сфотографированных с экрана. Разработанные методы предполагают минимальные визуальные изменения документов и обеспечивают сохранность внедренных ЦВЗ при искажениях, возникающих в процессе их передачи, в том числе, посредством мессенджеров. Это позволяет эффективно применять данные методы в системах защиты информации.

Актуальность темы

Активное использование информационных систем повышает риск утечек данных, особенно через так называемые «аналоговые» каналы – фотографирование или сканирование распечатанных документов, а также фотографирование документов, выведенных на экран. Утечки конфиденциальной информации, включая данные о клиентах или технологиях, способны нанести серьезный финансовый и репутационный ущерб организационным структурам. При этом большая часть (до 70-80%) подобных инцидентов связана с действиями внутренних нарушителей, что, в свою очередь, указывает на необходимость разработки более эффективных методов защиты. Существующие DLP-системы, как правило, неэффективны для защиты от утечек через аналоговые каналы.

Одним из перспективных решений выявленной проблемы является внедрение в документы водяных знаков, позволяющих идентифицировать источник утечки. Существующие подходы и практические решения на основе ЦВЗ имеют различные ограничения, как например, необходимость наличия оригинальной версии документа для извлечения ЦВЗ, высокая заметность ЦВЗ, поддержка алгоритмом внедрения ЦВЗ

ограниченного числа форматов документов и других. Для практического применения требуется учесть недостатки существующих решений и разработать методы внедрения малозаметных ЦВЗ, минимально изменяющих внешний вид документа и устойчивых к искажениям, возникающим при печати документов с последующей оцифровкой сканированием или фотографированием, при фотографировании выведенного на экран документа или сжатии изображений документов. В связи с этим, тема диссертации Д.О. Обыденкова, посвященной разработке и реализации системы защиты от анонимных утечек текстовых документов посредством ЦВЗ, является **актуальной.**

Структура и основное содержание диссертационной работы

Диссертация имеет общий объем 164 страницы и состоит из введения, пяти глав, заключения, списка литературы из 67 наименования, 48 рисунков, 24 таблиц и двух приложений.

Во введении обосновывается актуальность исследования, проводимого в рамках данной диссертационной работы, ставятся цели и задачи диссертационной работы, формулируется научная новизна и практическая значимость работы, а также приводятся основные положения, выносимые на защиту.

В первой главе представлен обзор опубликованных исследователями методов и существующих промышленных систем защиты от утечек информации на основе ЦВЗ, устойчивых к искажениям при печати и фотографировании экрана, а также описаны их ограничения;

Во второй главе описана архитектура системы деанонимизации при утечках, реализуемых путем фотографирования, текстовых документов, выводимых на печать или экран, с использованием методов внедрения ЦВЗ, содержащих уникальные идентификаторы сотрудников и их устройств.

В третьей главе описан разработанный структурный метод внедрения ЦВЗ с возможностью слепого извлечения. Метод основан на сегментации изображения документа с использованием нейросетевого алгоритма, устойчивого к искажениям, возникающим при печати и последующей оцифровке посредством сканирования или фотографирования. Нейросетевой алгоритм оптимизирован для работы на процессорах общего назначения с минимальными затратами вычислительных ресурсов.

В четвертой главе описан разработанный метод создания графического ЦВЗ на основе нейросетевого алгоритма для наложения на выводимое на экран изображение, обеспечивающий возможность слепого извлечения. Сгенерированный ЦВЗ характеризуется визуальной незаметностью и устойчивостью к искажениям, возникающим при фотографировании экрана и сжатии алгоритмами, применяемыми в мессенджерах при отправке изображений.

В пятой главе представлены результаты тестирования разработанных методов деанонимизации утечек текстовых документов с использованием ЦВЗ, поддерживающих слепое извлечение. Разработанные методы демонстрируют устойчивость к искажениям, возникающим при печати или фотографировании экранных документов с последующей передачей изображений через мессенджеры, а также отличаются визуальной незаметностью и не вызывают дискомфорта у пользователей.

В заключении перечислены основные результаты диссертационной работы.

Основные результаты диссертационной работы

В диссертационной работе Д.О. Обыденкова получены следующие основные результаты:

1. Разработана архитектура системы деанонимизации при утечках изображений текстовых документов, обеспечивающая внедрение уникальных идентификаторов сотрудников и используемых ими устройств в документы при печати и выводе на экран;
2. Разработан обладающий научной новизной структурный метод внедрения ЦВЗ, обеспечивающий слепое извлечение информации. Метод основан на нейросетевой сегментации изображений, обладает визуальной незаметностью, устойчивостью к искажениям при печати и оцифровке, и оптимизирован для работы на процессорах общего назначения с низкими вычислительными затратами;
3. Разработан метод генерации ЦВЗ нейросетевым алгоритмом, поддерживающий слепое извлечение, обладающий визуальной незаметностью и устойчивостью к искажениям, возникающим при фотографировании экрана и сжатии изображений мессенджерами.
4. На основе разработанных архитектуры и методов внедрения/извлечения ЦВЗ реализована система противодействия анонимным утечкам текстовых документов. Система протестирована на целевых сценариях утечек – фотографирование документов на экране и сканирование распечатанных документов. Апробация подтвердила эффективность системы в различных условиях, демонстрируя способность успешно извлекать внедренную в ЦВЗ информацию и деанонимизировать утечки.

Достоверность полученных результатов

Достоверность полученных результатов подтверждается экспериментальной и теоретической проверкой работоспособности предложенных подходов, в том числе с использованием разработанных программ для ЭВМ.

Теоретическая и практическая значимость

Теоретическая значимость диссертации заключается в разработке и усовершенствовании методов защиты текстовых документов от утечек информации через анонимные каналы с помощью ЦВЗ. В работе предложены новые решения, направленные на предотвращение несанкционированной передачи информации через печатные и отображаемые на экране документы, что расширяет научные представления в области внедрения ЦВЗ.

Практическая значимость полученных результатов состоит в том, что предложенный соискателем метод противодействия анонимности утечек текстовых документов посредством цифровых водяных знаков применен при реализации системы защиты информации. Тестирование реализованной в рамках работы системы показало, что точность извлечения ЦВЗ из фотографии или сканированного изображения распечатанного документа составляет более 80%. При наложении ЦВЗ на экран точность извлечения достигает 86.67% при непрозрачности водяного знака 8/255.

Реализованная система внедрена организацией ООО "СиТ" (акт о внедрении №612/0924 от 29.09.24).

Замечания по работе

При рассмотрении диссертации выявлен ряд замечаний:

1. В главе 1 недостаточно аргументирована непригодность работающих в домене преобразования методов внедрения ЦВЗ в изображения документов в рамках поставленной задачи;
2. В главе 2 описан механизм генерации идентификатора сотрудника и устройства, опирающийся на иерархию департаментов в организации. При этом было бы полезным определить механизм распределения сотрудников по департаментам и сценарий превышения расчетного размера департамента.
3. В главе 3 при сравнении производительности обученных нейросетевых моделей (таблица 3.3) с результатами сторонних инструментов текстовой сегментации (таблица 3.4) не учитывается время, необходимое на обработку результатов работы нейросетевой модели.
4. Формальное определение разметки текстового документа, введенное в главе 3, не учитывает необходимость разделения пикселей машинописного текста и пикселей, относящихся к фону, рукописным элементам, шумам и прочим.
5. В главе 4 не обоснован выбор размера базового изображения цифрового водяного знака.
6. В главе 5 при тестировании метода внедрения ЦВЗ в текстовые документы при печати с последующей оцифровкой фотографированием использована только одна пара устройств принтера и фотоаппарата.

Кроме того, имеются ошибки редакционного характера. Например, в тексте автореферата (с.21,22) ссылки на таблицы 4 – 7 не соответствуют содержанию и названию таблиц.

Вместе с тем, отмеченные недостатки не снижают в целом положительного впечатления от рецензируемой диссертационной работы, которая выполнена на достаточно высоком уровне и является законченным научным исследованием. Основные результаты диссертации опубликованы в 8 статьях автора, включая 4 из перечня ВАК, а также докладывались на конференциях.

Автореферат правильно и полно отражает содержание диссертации.

Заключение по работе

Диссертация Д.О. Обыденкова является законченной научно-квалификационной работой, в которой решена актуальная задача исследования и разработки методов противодействия анонимности при утечках текстовых документов посредством цифровых водяных знаков. Основные результаты диссертации в достаточной мере апробированы на профильных конференциях, опубликованы, в том числе в журналах из перечня ВАК, и корректно отражены в автореферате диссертации. Полученные результаты являются новыми, степень их обоснованности и достоверности является достаточной.

Таким образом, диссертационная работа «Методы противодействия анонимности при утечках текстовых документов посредством цифровых водяных знаков» отвечает критериям Положения о присуждении ученых степеней, утвержденного Постановлением Правительства РФ от 24.09.2013 г. №842, а ее автор Д.О. Обыденков заслуживает присуждения ученой степени кандидата технических наук по специальности 2.3.5 – Математическое и программное обеспечение вычислительных систем, комплексов и

компьютерных сетей.

Диссертационная работа и отзыв на диссертацию обсужден и единогласно одобрен на заседании секции Ученого совета ФИЦ ИУ РАН (протокол № 8 от 27 ноября 2024 г., присутствовало 11 членов секции, включая 5 докторов и 2 кандидата наук).

А. А. Зацаринный

«29» ноября 2024 г.

Александр Алексеевич Зацаринный - научный руководитель Отделения №5 «Информационные, управляющие и телекоммуникационные системы, информационная безопасность» ФИЦ ИУ РАН, главный научный сотрудник ФИЦ ИУ РАН, чл.-корр. Академии криптографии РФ, д.т.н. (05.13.15 - вычислительные машины, комплексы и компьютерные сети), профессор

Федеральное государственное учреждение «Федеральный исследовательский цент «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН)
Адрес: 119333, Москва, Вавилова, д. 44, кор. 2
http://www.frccsc.ru/
Тел: +7 (499) 135-62-60
E-mail: frccsc@frccsc.ru