DOI: 10.21778/2413-9599-2021-31-2-72-78
УДК 658.382.3

Проблемы обеспечения конфиденциальности документов в корпоративной информационной системе промышленного предприятия

А. Б. Лачихина[1], А. А. Петраков[2]

[1] ФГБОУ ВО «Московский государственный технический университет им. Н. Э. Баумана», Калужский филиал, Калуга, Россия
[2] АО «Научно-производственное предприятие «Калужский приборостроительный завод «Тайфун», Калуга, Россия

Постановка проблемы. В настоящее время вопрос контроля конфиденциальности информации в документах, создаваемых, обрабатываемых, передаваемых и хранящихся в корпоративной информационной системе после его открытия является одним из наиболее острых при обеспечении информационной безопасности промышленного предприятия.

Цель. Выявление рациональных способов предотвращения утечки электронных документов, распечатанных или открытых на экранах компьютеров корпоративной информационной системы.

Результаты. Приведены примеры классических методов защиты информации от нарушения ее конфиденциальности. Отмечена неэффективность подобных приемов для документов, открытых на экранах или распечатанных на бумаге. В качестве возможного механизма поддержания конфиденциальности корпоративной документации предложена маркировка. Рассмотрены современные технологии, предназначенные для маркирования электронных документов, предлагаемые на российском рынке средств защиты информации. Приведены принципы их работы, достоинства и недостатки. Проведенный анализ позволил сделать вывод о возможности применения рассмотренных технологий с целью расследования инцидентов утечки электронных или распечатанных документов и выявления нарушителей.

Практическая значимость. Высказано предположение о возможном косвенном влиянии применения маркировки электронных документов на снижение количества нарушений внутри корпоративной информационной системы.

Ключевые слова: конфиденциальность, маркировка, утечка информации, расследование инцидентов

Для цитирования:
Лачихина А. Б., Петраков А. А. Проблемы обеспечения конфиденциальности документов в корпоративной информационной системе промышленного предприятия // Радиопромышленность. 2021. Т. 31, № 2. С. 72–78. DOI: 10.21778/2413-9599-2021-31-2-72-78

© Лачихина А. Б., Петраков А. А., 2021

Problems of ensuring the confidentiality of documents in the corporate information system of an industrial enterprise

A. B. Lachikhina[1], A. A. Petrakov[2]

[1] Bauman Moscow State Technical University, Kaluga branch, Kaluga, Russia
[2] Research and Production Enterprise "Kaluga-based Instrument-Making Plant "TYPHOON" JSC, Kaluga, Russia

Problem statement. Currently, the issue of controlling the confidentiality of information in documents created, processed, transmitted and stored in the corporate information system (after of the documents open) is one of the most acute in ensuring the information security of an industrial enterprise.

The purpose. Detection of rational ways to prevent the leakage of electronic documents, which are printed or opened on the computer screens of the corporate information system.

Results. The article provides examples of classical methods for information protection from violation of its confidentiality. In the paper note the inefficiency of such techniques for opened on screens or printed documents. The authors propose labeling as a possible mechanism for maintaining the confidentiality of corporate documentation. There are considering modern technologies intended for marking of electronic documents, offered in the Russian market of information protection means. The principles of their work, advantages and disadvantages are given. The analysis allow drawing a conclusion about the possibility of considered technologies usage for investigation of electronic or printed documents leakage incidents and identifying violators.

Practical relevance. The authors suggested that electronic document labeling may affect (indirect) on reducing the number of violations within the corporate information system.

Keywords: confidentiality, marking, information leak, incident investigation

For citation:
Lachikhina A. B., Petrakov A. A. Problems of ensuring the confidentiality of documents in the corporate information system of an industrial enterprise. Radio industry (Russia), 2021: 31 (2); pp. 72–78. (In Russian). DOI: 10.21778/2413-9599-2021-31-2-72-78

Введение

За последние восемь-десять лет в практику управления промышленными предприятиями вошло такое направление, как менеджмент информационной безопасности [1]. Одной из проблем, связанных с защищенностью корпоративной информационной системы предприятия, является нарушение конфиденциальности документов, циркулирующих внутри системы.

Обеспечение конфиденциальности является наиболее хорошо проработанным аспектом информационной безопасности. К основным группам методов данного направления защиты информации относятся: криптографические методы, управление доступом к системе и ресурсам, предотвращение утечек информации по различным каналам. Они могут применяться независимо от типа предполагаемых нарушителей информационной безопасности. Статистика последних лет показывает, что наиболее часто возникают угрозы от внутренних нарушителей, при этом доступ к документам, как правило, разрешен многим сотрудникам.

Анализ проблемы

Управление доступом к информационным, программным и аппаратным ресурсам КИС является обычной практикой обеспечения конфиденциальности документации предприятия. Проблема контроля документа после открытия практически никем не решается.

Экран можно сфотографировать, бумажный документ можно ксерокопировать и отсканировать заново. Затем копия документа может быть распространена без малейшего риска для злоумышленника.

Для защиты документов в таких ситуациях существуют относительно простые и недорогие

методы. Одним из наиболее распространенных вариантов является уникальная идентификация и защита копии документа путем включения в ее содержание некоторых отличительных признаков. Этот метод принято называть маркировкой.

На российском рынке средств защиты информации наиболее известными технологиями маркировки документов с целью защиты от утечки информации из открытых документов являются технологии *SafeCopy, EveryTag* и *StegMark*.

Технологии маркировки документов

Технология *SafeCopy* предназначена для защиты компаний от рисков, связанных с несанкционированным распространением печатных и электронных копий документов. В ней используется запатентованный метод маркирования документов, который позволяет при возникновении инцидента провести расследование и определить возможный источник утечки информации.

Выявление канала утечки осуществляется путем идентификации скомпрометированных копий защищаемого документа в виде:

1. фотокопии с бумажного документа;
2. фотокопии с электронного документа;
3. фотокопии экрана, на котором открыт защищаемый документ;
4. отсканированного изображения бумажного документа;
5. электронной копии, в том числе фотографии (частичной или полной) документа.

С помощью *SafeCopy* для каждого получателя изготавливается уникальная копия документа [2].

При создании копии в нее автоматически вносятся невидимые для конечного пользователя изменения, реализуемые с использованием математического алгоритма на базе аффинных преобразований, модификаций межбуквенных и межстрочных интервалов. Главный плюс такой маркировки — ее нельзя убрать без изменения содержимого документа.

Оригинал документа хранится в базе для последующего сравнения и проведения расследований. В базе данных *SafeCopy* хранится не полная копия документа, а только уникальная совокупность маркировочных признаков, по которым *SafeCopy* при обращении восстанавливает полную копию. В результате объем базы *SafeCopy* не зависит от числа изготавливаемых копий документов.

Принцип технологии представлен на *рис. 1*.

Рис. 1. Технология SafeCopy
Fig. 1. SafeCopy technology

Копии выдаются получателям в печатном виде или в электронном *pdf*-формате. В случае утечки копии можно гарантированно определить его получателя по уникальной совокупности искажений, вносимых в каждую копию. Поскольку маркируется весь текст, для этого достаточно буквально нескольких абзацев.

Логику работы решения проще всего описать с помощью возможных сценариев работы.

1. На рабочих местах пользователей настраивается виртуальный принтер; при отправке на него документов производится их автоматическая маркировка с помощью *SafeCopy*.

2. Секретарь загружает документы в веб-интерфейс *SafeCopy*, запрашивает изготовление копий для получателей, после чего получатели забирают копии из принтера с авторизацией на нем (например, по *RFID*-метке), если принтер поддерживает такую авторизацию.
3. Система управления печатью распознает среди документов, отправляемых пользователями на печать, те, которые подлежат маркировке, и запрашивает у *SafeCopy* изготовление маркированных копий перед формированием задания на печать на одном из принтеров, которыми она управляет.

Достоинства:

1) централизованное хранение, учет и управление оборотом корпоративных документов, не подлежащих распространению;
2) защита от несанкционированного распространения конфиденциальных документов;
3) выявление канала утечки документа по его скриншоту, фотографии (в том числе сделанной под отличным от 90 ° углом);
4) возможность проведения расследований по фотографиям низкого качества, которые, например, получаются в результате пересылки с помощью мессенджеров;
5) изготовление копий, визуально неотличимых от оригинала документа, с помощью аффинных преобразований;
6) возможность использования маркировки для проверки подлинности документов или бланков строгой отчетности (паспорта, водительские права, билеты, страховые полисы, заявления в органы власти и др.);
7) защита вложений электронной почты;
8) успешный опыт внедрения в информационные системы крупных промышленных компаний.

Недостатки:

1) отсутствие в эксплуатационной документации четких рекомендаций по наиболее эффективному определению области распознавания копии документа и по расстановке меток при проведении расследования инцидента.

Система *SafeCopy* гарантирует защиту компаний различного профиля от рисков, связанных с несанкционированным распространением печатных и электронных копий документов с целью передачи конкурентам, представителям прессы и т. д.

В основе технологий EveryTag лежит запатентованный алгоритм маркировки, который создает уникальную копию изображения информации для каждого сотрудника компании [3]. Принцип работы технологии представлен на *рис. 2*.

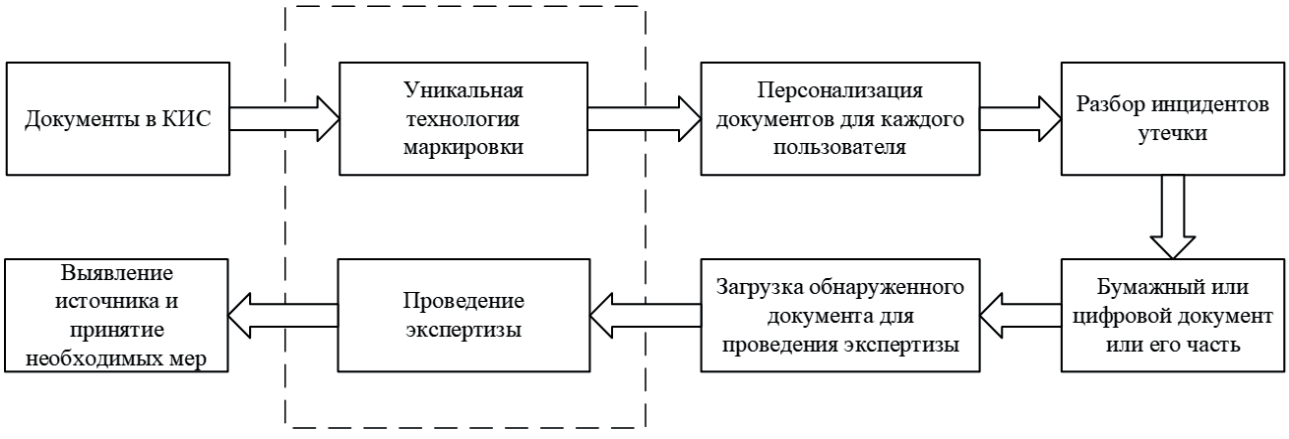

Рис. 2. Технология EveryTag
Fig. 2. EveryTag technology

Требующие защиты документы предприятия размещаются в специальном защищенном хранилище. При каждом открытии документа на экране или выводе его на печать системой создается уникальная копия, трансформированная в соответствии со специальным алгоритмом. Иными словами, пользователю предоставляется не сам документ, а персонализированная копия, на основе которой можно выяснить информацию о лице, получившем ее.

В созданные копии не внедряются специальные символы или метки, так как они могут быть заменены или удалены при обнаружении. Но в каждой строке документа размещается информация, привязанная к получателю копии.

В результате работы уникального алгоритма разделенный на блоки и переведенный в определенный формат документ служит основой для выработки псевдослучайной последовательности.

Алгоритм преобразования позволяет для одной страницы А4 создать 27 тысяч уникальных копий. В случае обнаружения утечки документа за пределы предприятия можно воспользоваться специальными средствами для проведения расследования, встроенными в систему *EveryTag*. К таким инструментам относятся:

1) механизм поиска скомпрометированного документа по образцу, атрибутам или смысловому тексту;
2) механизм анализа образца и исходного документа на предмет идентификации персонализированной копии.

Инструменты предназначены для эксперта, который на основе результатов их работы может сделать вывод о степени соответствия полученного образца и копиями документа в системе. В случае их совпадения устанавливается, для какого пользователя была изготовлена копия документа. Что в свою очередь дает возможность предположить, кто является возможным нарушителем.

Достоинства:

1) наличие собственного запатентованного алгоритма преобразования документы для создания уникальных копий;
2) возможность создания огромного количества уникальных копий документов;
3) отсутствие необходимости хранения созданных копий документов (хранятся исходный документ и уникальные комбинации алгоритмов преобразований);
4) наличие инструментов проведения расследования, позволяющего выявить нарушителя с высокой долей вероятности (соответственно, создание «неотвратимости наказания»).

Недостатки:

1) необходимость участия эксперта в процессе расследования в связи с отсутствием полной автоматизации данных механизмов;
2) возможность использования только в текстовых документах (невозможно использовать в электронных письмах, базах данных).

Несмотря на достаточно ограниченную сферу применения технология *EveryTag* является полезным средством в сфере защиты конфиденциальности открытых на экране и распечатанных документов.

Технология *StegMark* — это программный продукт для модификации электронных отсканированных документов в момент их скачивания из архива и их дальнейшего распознавания. Система предназначена для проведения расследования утечки конфиденциальных документов на предприятии, в частности для выявления виновного в распространении документов ограниченного доступа.

Система для каждого сотрудника компании осуществляет внешне незаметную модификацию интервалов (межбуквенных, между словами, межстрочных) в скан-копии исходного документа. Модификация интервалов производится в момент, когда пользователь системы электронного документооборота открывает файл «на чтение» из электронного архива [5].

Файлы модифицируются уникальным для каждого сотрудника организации образом, в дальнейшем, в случае инцидента, имея на руках незаконно попавшую вовне копию такого документа, достаточно запустить его скан-копию на анализ в системе, чтобы на выходе получить уникальный идентификатор пользователя, скачавшего документ из электронного архива компании.

Принцип технологии представлен на *рис. 3*.

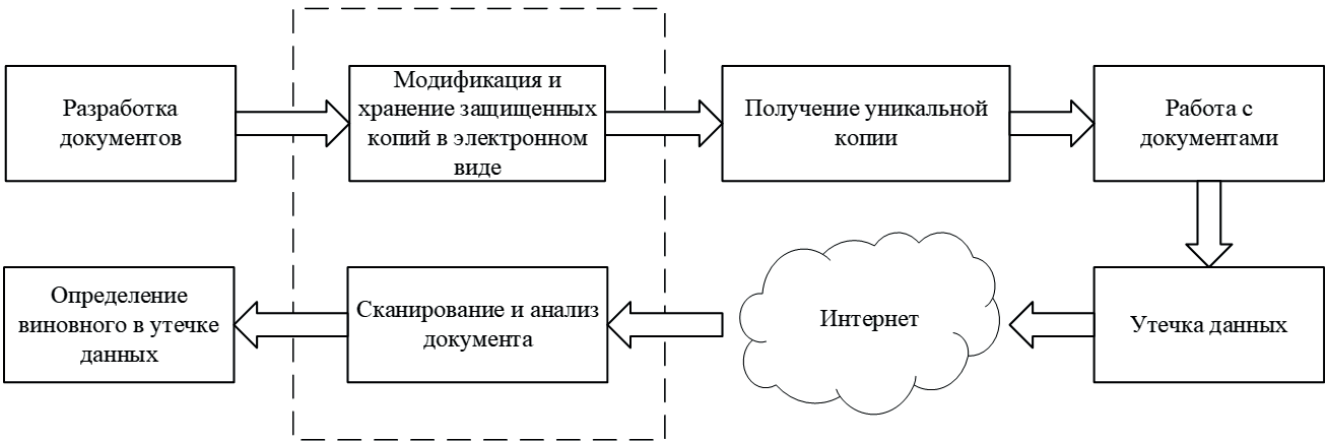

Рис. 3. Технология StegMark
Fig. 3. StegMark technology

Достоинства:

1) использует нейронную сеть. За счет использования ИНС для распознавания содержимого документа обеспечивается больше вариантов маркировки документов, модификация любого документа, с минимальным количеством строк, любым шрифтом;
2) интеграция с любой ИС. Решение интегрируется с любой информационной системой заказчика, в которой хранятся конфиденциальные документы компании.

Современные компании накапливают и обрабатывают большие объемы данных. Соответствующие технологические процессы предполагают создание множества печатных и электронных документов, а также интенсивный обмен ими. В рамках этого информационного обмена особое место отводится конфиденциальным корпоративным документам, которые нуждаются в эффективной защите.

Для защиты документов от копирования и незаконного распространения, а также для сохранения авторских прав используется технология маркирования документов. Применяются как видимые (за счет внесения в предназначенный для печати документ незначительных изменений), так и скрытые (за счет внедрения цифровых знаков в файл документа) признаки маркировки. В результате выданные пользователям персональные копии документа минимально отличаются друг от друга и от оригинала, но эти отличия достаточны для того, чтобы при возникновении инцидента можно было с высокой вероятностью определить, чья именно копия была скомпрометирована.

В результате анализа запатентованных технологий защиты информации открытых документов был сделан вывод, что не существует универсального решения, подходящего для всех корпоративных информационных систем. В *табл. 1* приведены основные характеристики рассмотренных технологий маркировки.

Таблица 1
Table 1
Сравнительная характеристика технологий маркировки
Comparative analysis of the marking technologies

	SafeCopy	Everytag	StegMark
Алгоритм маркировки	Аффинные преобразования	Собственный алгоритм	Нейронная сеть
Вид документов для маркировки	Любой	Текстовые документы	Любой
Защита от НСД	Да	Да	Да
Возможность внедрение в ИС	В любую	В небольшую компанию	В любую
Автоматизация процесса	Полная	Необходим эксперт	Полная
Хранение копий	Хранение не полных копий	Нет хранения	Есть хранение

Опыт зарубежных ученых, отраженный в научных публикациях международной базы цитирования *Scopus*, показывает, что разработки ведутся в тех же направлениях, что и российскими учеными, в частности, предлагаются различные стеганографические методы [6–9].

Выводы

Возможным решением проблемы утечки электронных документов мог бы стать комплексный продукт, объединяющий сильные стороны рассмотренных технологий. Следует также отметить, что ни одно из рассмотренных средств не защищает информацию от утечки. Тем не менее пренебрегать их использованием не стоит, так как они позволяют проводить расследование инцидентов и выявлять нарушителей, что, в свою очередь, способствует снижению количества нарушений.

ПРИСТАТЕЙНЫЙ БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Лачихина А. Б., Петраков А. А.* Подходы и методы управления информационной безопасностью в процессе управления промышленным предприятием // Вопросы радиоэлектроники. 2017. № 11. С. 48–51.
2. Защита документов от копирования [Электронный ресурс] // Блог компании НИИ СОКБ : сайт. URL: https://habr.com/ru/company/niisokb/blog/511320/ (дата обращения: 03.05.2021).
3. Принципы работы технологии EveryTag // ЭвриТег» : сайт. URL: https://everytag.ru/ (дата обращения: 03.05.2021).

4. *Хонин А.* Обзор Everytag Information Leaks Detection (ILD) — системы контроля и защиты документов // Anti — Malware : сайт. URL: https://www.anti-malware.ru/reviews/everytag-information-leaks-detection-ild/ (дата обращения: 03.05.2021).
5. Защита конфиденциальных документов компании от несанкционированного распространения // CorpSoft24 : сайт. URL: https://www.corpsoft24.ru/it/stegmark/ (дата обращения: 03.05.2021).
6. *Kozachok A. V., Kopylov S. A., Shelupanov A. A., Evsutin O. O.* Text marking approach for data leakage prevention. Text marking approach for data leakage prevention // J Comput Virol Hack Tech. 2019. No. 15. Pp. 219–232. DOI: 10.1007/s11416-019-00336-9.
7. *Lopez G., Richardson N., Carvajal J.* Methodology for data loss prevention technology evaluation for protecting sensitive information // Revista Politécnica. 2015. Vol. 36. No. 3.
8. *Pamulaparty L., Rao N. M.* Text Steganography: Review // International Journal of Computer Science and Information Technology & Security (IJCSITS). 2016. Vol. 6. No. 4. Pp. 80–83.
9. *Woo C. S.* Digital Image Watermarking Methods for Copyright Protection and Authentication. Brisbane : Queensland University of Technology, 2007.

REFERENCES

1. Lachikhina AB, Petrakov AA. The approaches and methods of information security management in enterprise management process. *Voprosy radioelektroniki*, 2017;11:48–51. (In Russian).
2. *Zashchita dokumentov ot kopirovaniya* [Copyprotection of documents]. *NII SOKB company blog.* (In Russian). Available at: https://habr.com/ru/company/niisokb/blog/511320/ (accessed: 03.05.2021).
3. *Printsipy raboty tekhnologii EveryTag* [Operating principles of EveryTag technology]. *EvriTag Website.* (In Russian). Available at: https://everytag.ru/ (accessed: 03.05.2021).
4. Khonin A. *Obzor Everytag Information Leaks Detection (ILD) — sistemy kontrolya i zashchity dokumentov* [Everytag Information Leaks Detection (ILD) Review – the documents control and protection systems]. Anti — Malware: electronic edition. (In Russian). Available at: https://www.anti-malware.ru/reviews/everytag-information-leaks-detection-ild (accessed: 03.05.2021).
5. *Zashchita konfidentsialnykh dokumentov kompanii ot nesanktsionirovannogo raspro-straneniya* [Protection of a company confidential documents from unauthorized distribution]. CorpSoft24 website. (In Russian). Available at: https://www.corpsoft24.ru/it/stegmark/ (accessed: 03.05.2021).
6. Kozachok AV., Kopylov SA., Shelupanov AA., Evsutin OO. Text marking approach for data leakage prevention. Text marking approach for data leakage prevention. *J Comput Virol Hack Tech*, 2019;15:219–32. DOI: 10.1007/s11416-019-00336-9.
7. Lopez G, Richardson N, Carvajal J. Methodology for data loss prevention technology evaluation for protecting sensitive information. *Revista Politécnica*, 2015; 36(3), 69
8. Pamulaparty L, Rao NM. Text Steganography: Review. *International Journal of Computer Science and Information Technology & Security (IJCSITS)*, 2016;6(4):80–3.
9. Woo CS. *Digital Image Watermarking Methods for Copyright Protection and Authentication.* Brisbane, Queensland University of Technology, 2007.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Лачихина Анастасия Борисовна, к. т. н., доцент, ФГБОУ ВО «Московский государственный технический университет им. Н. Э. Баумана», Калужский филиал, 248000, г. Калуга, ул. Баженова, д. 2, e-mail: anastaisalach73@gmail.com.

Петраков Андрей Алексеевич, генеральный директор, АО «Научно-производственное предприятие «Калужский приборостроительный завод «Тайфун», 248009, г. Калуга, ул. Грабцевское шоссе, д. 174, e-mail: info@typhoon-jsc.ru.

AUTHORS

Anastasiya B. Lachikhina, PhD (Engineering), associate professor, Bauman Moscow State Technical University, Kaluga branch, 2, ulitsa Bazhenova, Kaluga, 248000, Russia, e-mail: anastasialach73@gmail.com.

Petrakov Andrey, CEO, Research and Production Enterprise “Kaluga-based Instrument-Making Plant “TYPHOON” JSC, 174, Grabtsevskoe shosse, Kaluga, 248009, Russia, e-mail: info@typhoon-jsc.ru.

Поступила 12.03.2021; принята к публикации 03.05.2021; опубликована онлайн 28.06.2021.
Submitted 12.03.2021; revised 03.05.2021; published online 28.06.2021.