ОСОБЕННОСТИ И ПЕРСПЕКТИВЫ ТЕХНОЛОГИИ EVERYTAG ДЛЯ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНЫХ ДОКУМЕНТОВ

В. В. Вавуло, М. С. Солодухо

ГУО «Институт бизнеса Белорусского государственного университета», г. Минск
valerie.vers@mail.ru; mariyasolodukho@gmail.com;
науч. рук. – Т. А, Ермакова, канд. экон. наук, доц.

Статья посвящена аналитическому исследованию технологии EveryTag для защиты конфиденциальных документов и выявления мошенников. В процессе исследования были рассмотрены предпосылки и основные причины востребованности данной технологии, её особенности, перспективы развития, а также проанализированы преимущества и недостатки.

Ключевые слова: технология EveryTag; утечки данных; система электронного документооборота.

Цифровизация экономики помимо очевидной для всех пользы привносит и дополнительные риски, связанные с защитой информации. Использование популярных на рынке методов и средств защиты информации, к сожалению, не дает должного эффекта – утечки конфиденциальных документов и баз данных происходят с завидным постоянством [1].

Проблема состоит в том, что контролируются операции с файловыми объектами внутри корпоративного периметра или за его пределами. Доступ к конфиденциальному документу может быть у целой группы сотрудников, и зачастую крайне сложно обнаружить виновника. Ранее считалось, что главную опасность для корпоративных систем представляют злоумышленники, проникающие в них извне. Теперь же становится очевидным, что наибольший вред способны нанести бизнесу люди изнутри: собственные сотрудники, клиенты, партнеры – все, кто имеет доступ к конфиденциальной информации. За период 2020–2021 гг. на основе публичных сообщений выявлено 24,4 тысячи записей, в результате утечки которых были скомпрометированы персональные данные белорусских граждан. Процентное количество утечек по вине сотрудников представлено на рисунке 1.

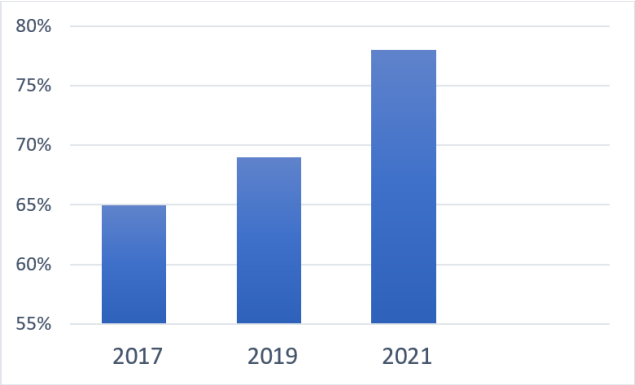

Рис. 1. Процент утечек по вине сотрудников

В 2020–2021 гг. экспертно-аналитическим центром InfoWatch зарегистрировано 22 случая утечки информации ограниченного доступа из белорусского госсектора и коммерческих компаний. За два года в 40 % случаев утечки информации были спровоцированы действиями внешних нарушителей, в 60 % – внутренних, что графически представлено на рисунке 2 [2].

Рис. 2. Вид информации. Причины утечки

В условиях пандемии COVID-19, когда значительная часть работников была переведена на удалённый режим, особо обострилась проблема утечки конфиденциальных документов. В таблице ниже представлены основные причины утечек информации, произошедших по вине сотрудников [3].

Таблица 1

Основные причины утечек информации, произошедших по вине сотрудников

Процент утечек	Причина утечек
61 %	Происходит из-за недосмотра, т.е. сотрудники безответственно относились к защите и хранению конфиденциальных данных.
39 %	Фотографирование экрана, отправка фотографий через мессенджер, почту, облачные сервисы.

Российская компания Every Tag предлагает решение этой проблемы на основе оригинального запатентованного алгоритма. Не нужно обу-

чаться или менять схему работы с документами. Сотрудники получают документы по привычному алгоритму и все также используют необходимые в работе веб-сервисы. Они могут даже не знать, что система внедрена в компании. Продукт имеет юридическую значимость, результаты, полученные в процессе расследования, могут быть использованы в суде.

Принцип работы, вне зависимости от формата документа, довольно прост: каждый раз, когда пользователь видит информацию на экране или выводит её на печать, алгоритм системы показывает ему индивидуальную копию. Алгоритм создаёт уникальную маркировку документа при каждом обращении к нему. Другими словами, производится форматирование документа, незаметное для человека.

Система запоминает уникальный ключ, с помощью которого можно определить любые данные получателя.

Система определит злоумышленника, если произошла утечка. Если в открытых источниках обнаруживается несанкционированная копия, достаточно загрузить её в систему, чтобы вычислить злоумышленника.

Существует четыре основных продукта компании EveryTag, которые представлены в таблице 2.

Таблица 2

Основные продукты компании EveryTag

Название	Основное направление действия
EveryTag ILD (Information Leaks Detection)	Определение виновника утечки из системы документооборота, при пересылке файла по электронной почте или выводе на печать. Доступ к интерфейсу EveryTag получают только специалисты по безопасности.
EveryTag VDR (Virtual Data Room)	Виртуальная комната, среда, предназначенная для безопасного обмена документами. Работает аналогично Google.Drive или Яндекс.Диск и представляет собой пространство, в которое можно загружать важные документы и устанавливать разный уровень доступа к ним.
EveryTag UI (Unique Interface)	Маркировка интерфейсов при интеграции с веб-ориентированными системами. Защита информацию на экране от снятия скриншотов или простого фотографирования на смартфон.
EveryTag Fake ID (продукт находится в разработке)	Защита от подделки документов и проверка подлинности. Работает с любыми документами, содержащими текст.

Достоинства технологии:

- Система имеет собственный запатентованный алгоритм преобразования текста.
- Система внесена в Единый реестр белорусских программ для электронных вычислительных машин и баз данных как «Модуль для маркировки и выявления совпадающих печатных форм документов».

- Количество копий, которые создаются в процессе преобразования документов, практически неисчерпаемо.
- Система поддерживает несколько вариантов внедрения. Позволяет проводить расследование, по результатам которого гарантированно будет выявлен нарушитель.
- Работает там, где стандартные средства защиты не способны проконтролировать безопасность информации.

Недостатки технологии:

- Процесс расследования не является полностью автоматизированным и требует участия эксперта.
- Система применима только к документам, в которых содержатся какой-либо текст (в отношении электронных писем, баз данных представленная система уже не применима).

Информация давно перестала быть просто необходимым для производства вспомогательным ресурсом. Она приобрела ощутимый стоимостный вес [4]. Можно сказать, что не существует одного абсолютно надежного метода её защиты. Наиболее полную безопасность можно обеспечить только при комплексном подходе к этому вопросу.

Библиографические ссылки

1. Независимый информационно-аналитический центр по информационной безопасности [Электронный ресурс] / – Режим доступа: https://www.anti-malware.ru/reviews/everytag-information-leaks-detection-ild. – Дата доступа: 17.03.2022.
2. Сайт компании InfoWatch [Электронный ресурс] / – Режим доступа: https://www.infowatch.ru/company/presscenter/news/personalnye-dannye-grazhdan-belorussii-okazalis-pod-ugrozoy. Дата доступа: 22.03.2022.
3. Защита от утечки конфиденциальных документов. Обзор решений EveryTag [Электронный ресурс]. – Режим доступа: https://www.tadviser.ru/index.php. – Дата доступа: 18.03.2022.
4. Электронная библиотека Studbooks [Электронный ресурс]. – Режим доступа: https://studbooks.net/2224555/informatika/vvedenie. – Дата доступа: 20.03.2022.