

The logo for EveryTag, featuring a stylized white 'E' with a location pin icon inside, followed by the word 'EVERYTAG' in a bold, white, sans-serif font. The logo is set against a green triangular background that points downwards.

EVERYTAG

Защитите свою конфиденциальную информацию от утечек при фотографировании, копировании или печати с помощью запатентованной технологии невидимой маркировки EveryTag.

Один из критических моментов в ИБ — утечки, совершаемые самими **сотрудниками** компании.



79.1%

утечек информации в **российских** компаниях происходит именно по вине сотрудников.

* Отчёт InfoWatch за 2020 год

В отличие от внешних злоумышленников инсайдеры уже имеют доступ к конфиденциальной информации и могут ее в любой момент распечатать, забрать с собой или сделать фото на личный смартфон.



Технология

В основе технологии EveryTag лежит запатентованный алгоритм маркировки, который создает уникальную копию документа для **каждого сотрудника** компании или контрагента.

ID: Ivan Ivanov

Логин: Ivanov_I

Время: 17:42 (GMT +3)

IP: 136.0.16.217

Дата: 21/01/2020

Mac: 8c:8590:a9:f8:42

Должность: специалист

Отдел: Operation

Локация: Москва



Принцип работы технологии EveryTag



Когда пользователь обращается к документу, система создаёт уникальную копию.



Пользователь работает с уникальной версией отображенной информации.



Если произошла утечка, система определит источник по скомпрометированной копии.

205 891 136 094 649

уникальных комбинаций одной страницы текста формата А4 возможно создать благодаря маркировке

- Интеграция на уровне API
- Любые типы документов
- Разбор инцидента утечки
- Проведение экспертизы
- Гарантированное выявление источника утечки документов

Ситуации, в которых технология EveryTag помогает вычислить источник утечки:



Когда похищается информация в распечатанном виде



Когда делается фотография или скриншот экрана монитора с ценной информацией



Когда фотографируется распечатанный документ

Нам доверяют



ДЕПАРТАМЕНТ
ИНФОРМАЦИОННЫХ
ТЕХНОЛОГИЙ
ГОРОДА МОСКВЫ



Ростех



ГАЗПРОМ
НЕФТЬ



ПОЛЮС



Транснефть



МИНИСТЕРСТВО НАУКИ
И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ



РОСНЕФТЬ



Селигдар
ПУБЛИЧНОЕ АКЦИОНЕРНОЕ ОБЩЕСТВО



ФОСАГРО
АПАТИТ



ДИАЛОГ
РЕГИОНЫ



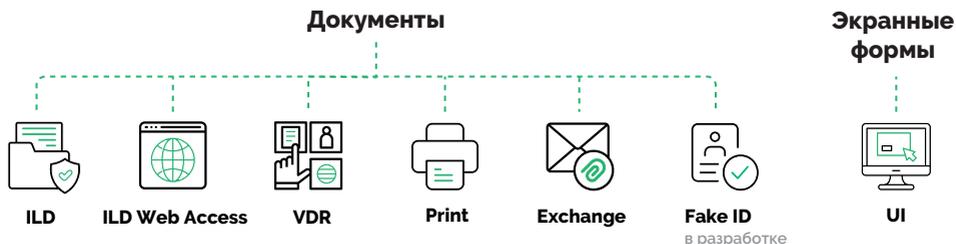
CAPITAL GROUP



МОСЭНЕРГО

Продуктовая линейка EveryTag

На базе технологии EveryTag представлено **7 продуктов** с разными функциональными характеристиками.



EveryTag ILD

Маркировка документов и определение источника утечки данных из систем документооборота

ILD (Information Leaks Detection) представляет собой инструмент для расследования и выявления источника утечки конфиденциальных данных из системы документооборота.

ILD бесшовно встраивается в документооборот компании и способен распознать документы во многих стандартных офисных форматах:



Возможны интеграции с СЭД: TESSA, ТЕЗИС, IBM FileNet, Directum, Documentum. Через REST API — в любые другие СЭД.

Копия визуально не отличается от оригинала, но обогащается маркировкой и содержит информацию о том, кто открыл документ, когда, на каком устройстве и пр.

- Интегрируйте ILD в существующую систему документооборота;
- Работайте с документами так, как вы привыкли (не требуется дополнительно настраивать доступы и проводить тренинги для сотрудников);
- Пользователь получит персональную маркированную копию документа каждый раз, когда будет открывать его;
- В случае утечки в ILD для проведения расследования загружается скомпрометированный файл:
 - Оригинал или фото **печатного документа**;
 - **Фото или скриншот экрана**, подойдет даже искаженный образец (помятый, загрязненный или повернутый под углом).



EveryTag ILD Web Access

Инструмент, позволяющий маркировать документы из веб-приложений различных систем прямо на лету за считанные секунды и не требующий сложной интеграции.



Не требует сложной интеграции, срок настройки – не более 7 дней.



Позволяет обеспечить незаметные для пользователя изменения при работе с документами.



Легко встраивается в маршрут любого веб-приложения, работающего с документами.

Защита информации с использованием технологии EveryTag ILD Web Access

- Взаимодействие с веб-ориентированными системами без изменения привычных процессов.
- ILD Web Access осуществляет маркировку на лету и выдает пользователям PDF-файлы.
- При подключении ILD Web Access не требуется изменение состояния целевой системы.

ILD Web Access подключается путем настройки в течение нескольких дней. Возможно быстрое включение и выключение инструмента без дополнительных финансовых затрат со стороны заказчика на сложное внедрение.



EveryTag VDR

VDR (Virtual Data Room) — это виртуальная комната, среда, предназначенная для безопасного обмена документами. VDR работает аналогично Google.Drive или Яндекс.Диск и представляет собой пространство, в которое можно загружать важные документы и устанавливать разный уровень доступа к ним.

- Загружайте документы в VDR.
- Настраивайте доступ и делитесь документами (по умолчанию каждый загружаемый в VDR документ доступен только его создателю и больше никому (в том числе нам).
- Пользователь получит персональную маркированную копию документа каждый раз, когда будет открывать его.

Варианты использования VDR — проведение критически важных деловых мероприятий; сделок по слиянию-поглощению, аудиторских проверок, подготовок к IPO и др.

Преимущества EveryTag VDR



Интеграция с другими системами



Работа с любого устройства



Доступ через браузер с любого рабочего места



EveryTag Print

Маркировка (модификация) копий защищенных документов при отправке на печать с использованием сервера печати (например, Microsoft Print Server).

Система поддерживает маркирование копий документов, которые отправляются на печать с использованием протокола IPP.

Print выполняет маркировку документа, отправленного на печать. Завершив процесс маркировки, Print отправляет модифицированную копию документа в очередь печати того принтера, который соответствует виртуальному принтеру, на который было отправлено оригинальное задание на печать.

- Никаких агентских приложений на автоматизированном рабочем месте (АРМ) пользователя не устанавливается.
- Принтеры устанавливаются на рабочих станциях через политики домена.

Любой подключенный к серверу печати принтер может быть использован системой для печати маркированных копий документов.

Форматы данных, поддерживаемые системой при отправке на печать:



EveryTag Exchange

Маркировка почтовых вложений с помощью почтового сервера Microsoft Exchange.

Процесс работы:

- 1 Каждое письмо, в которое вкладывается конфиденциальный документ, помечается отправителем в соответствии с заранее сделанными правилами настройки почтового сервера.
- 2 В этом случае функционал EveryTag перехватывает такое сообщение, формирует уникальную копию и от имени отправителя предоставляет письмо с новым вложением почтовому серверу для дальнейшей отправки.
- 3 Адресат, открывая почтовое вложение, обработанное таким способом, визуально не может заметить внесенные изменения.

При обработке извлекаются все вложения в сообщении, после этого вложения разделяются на поддерживаемые и неподдерживаемые форматы.

Вложения поддерживаемых форматов направляются для маркировки.

Далее для каждого вложения подготавливается набор копий по количеству адресатов в оригинальном сообщении.



EveryTag UI

Решение UI (Unique Interface) предназначено для установления источника утечки данных с экрана компьютера. UI маркирует веб-интерфейс с помощью алгоритма EveryTag, делая его уникальным для каждого пользователя.

Расследование утечек проводится специалистом по безопасности таким же образом, как и в случае с ILD, а образцом может служить как фото экрана, так и скриншот или его фрагмент.

Прозрачное встраивание в бизнес процессы

Все данные остаются в тех системах, программах и папках, в которых были до внедрения системы UI. Нет необходимости специально запускать работу алгоритма или переносить информацию в отдельные защищенные папки.

Влияние факторов на результат экспертизы

На успешное проведение экспертизы не могут повлиять ни разница в разрешении экрана, ни особенности рендеринга страницы для данного устройства, ни класс устройства отображения: монитор десктопа или ноутбука, планшета или смартфона.

UI защищает любую открытую на экране информацию:



Информацию из CRM или биллинговых систем



Данные из систем учёта, отчётности и аналитики



Данные из систем разработки и создания продуктов

Архитектура решения EveryTag

Кроссплатформенное решение EveryTag базируется на платформе Java Spring Boot и Quarkus и способно работать в различных операционных системах, в том числе и в гетерогенной среде. Решение может быть развернуто как на локальных серверах заказчика, так и в облачной среде.

Микросервисная архитектура позволяет разворачивать продукты EveryTag в сжатые сроки. Благодаря этому, все предлагаемые решения остаются гибкими в настройке и максимально отказоустойчивыми.

Поддерживаются режимы высокой доступности и отказоустойчивости. Системой хранения данных выступает документоориентированная (NoSQL) СУБД с открытым исходным кодом MongoDB с поддержкой вертикального и горизонтального масштабирования.

В роли файлового хранилища может использоваться как локальная, так и сетевая распределённая файловая система или S3 совместимый сервис. Данные в ней могут шифроваться с использованием различных алгоритмов (в том числе в соответствии с ГОСТом).

Взаимодействие с пользователем осуществляется по протоколу HTTPS с шифрованием трафика по стандартам SSL/TLS с SSL-сертификатами любого типа.

Веб-интерфейс доступен в браузерах Google Chrome, Opera, Edge, Safari и Firefox.

В продуктах EveryTag поддерживается интеграция с любым типом корпоративного LDAP-каталога для аутентификации пользователей или служб. Кроме того, в них реализованы аутентификация и авторизация на базе сервиса KeyCloak, обеспечивающего безопасное хранение учетных данных и настройку механизма однократной аутентификации для всех сервисов SSO (Single-Sing-On).

Авторизация и аутентификация

Модели разграничения доступа:

- Ролевая: RBAC – Role Based Access Control.
- Поддерживает интеграцию с LDAP-каталогом.
- Объективная: списки доступа ACL – Access Control List.
- Аутентификация на основе сервиса KeyCloak.
- Федеративное использование аутентификации.
- Kerberos MS.

Печать документов

- Маркированная печать с применением протокола IPP.
- Сервер печати по умолчанию – Microsoft Print Server.
- Поддерживаемые форматы данных для печати: PCL, PDF, XPS.
- Почтовый сервер по умолчанию – Microsoft Exchange Server.

Передача документов

- Взаимодействие с пользователем по протоколу HTTPS.
- Шифрование трафика по стандартам SSL/TLS.

Микросервисы



Хранилище данных



В решениях EveryTag применяются две модели разграничения доступа: ролевая (RBAC – Role Based Access Control) с назначением каждой роли набора полномочий, причём пользователь или группа из LDAP-каталога могут быть связаны с одной или несколькими ролями; и объектная на базе списков доступа (ACL – Access Control List), содержащих разрешения или запреты на определённые действия над конкретными объектами (папками и документами), с поддержкой отключаемого наследования и ограничения по срокам действия записей.

Продукты компании EveryTag внесены в реестр российского ПО Минкомсвязи РФ за рег. номером ПО 4464 согласно Приказу Минкомсвязи России от 12.04.2018 №157, рег. номером ПО 11299 согласно Приказу Минкомсвязи России от 13.08.2021 №830 и рег. номером ПО №11257 согласно Приказу Минкомсвязи России от 05.08.2021 №807 и рекомендованы к использованию российским компаниям и госучреждениям.

Функциональные возможности технологии EveryTag позволяют:

- Исключить анонимность и безнаказанность.
- Прозрачно встроить возможности системы в существующие бизнес-процессы.
- Работать со многими форматами файлов, содержащими важную информацию.
- Контролировать как зарегистрированных в системе пользователей, так и приглашенных внешних партнёров.

Уникальный механизм маркировки запатентован и является неотъемлемой частью технологии EveryTag, В компании задействованы ключевые эксперты российского рынка информационной безопасности, имеющие более чем 15-летний опыт работы на рынке. Экспертиза команды EveryTag выросла из проектов крупнейших российских компаний.

