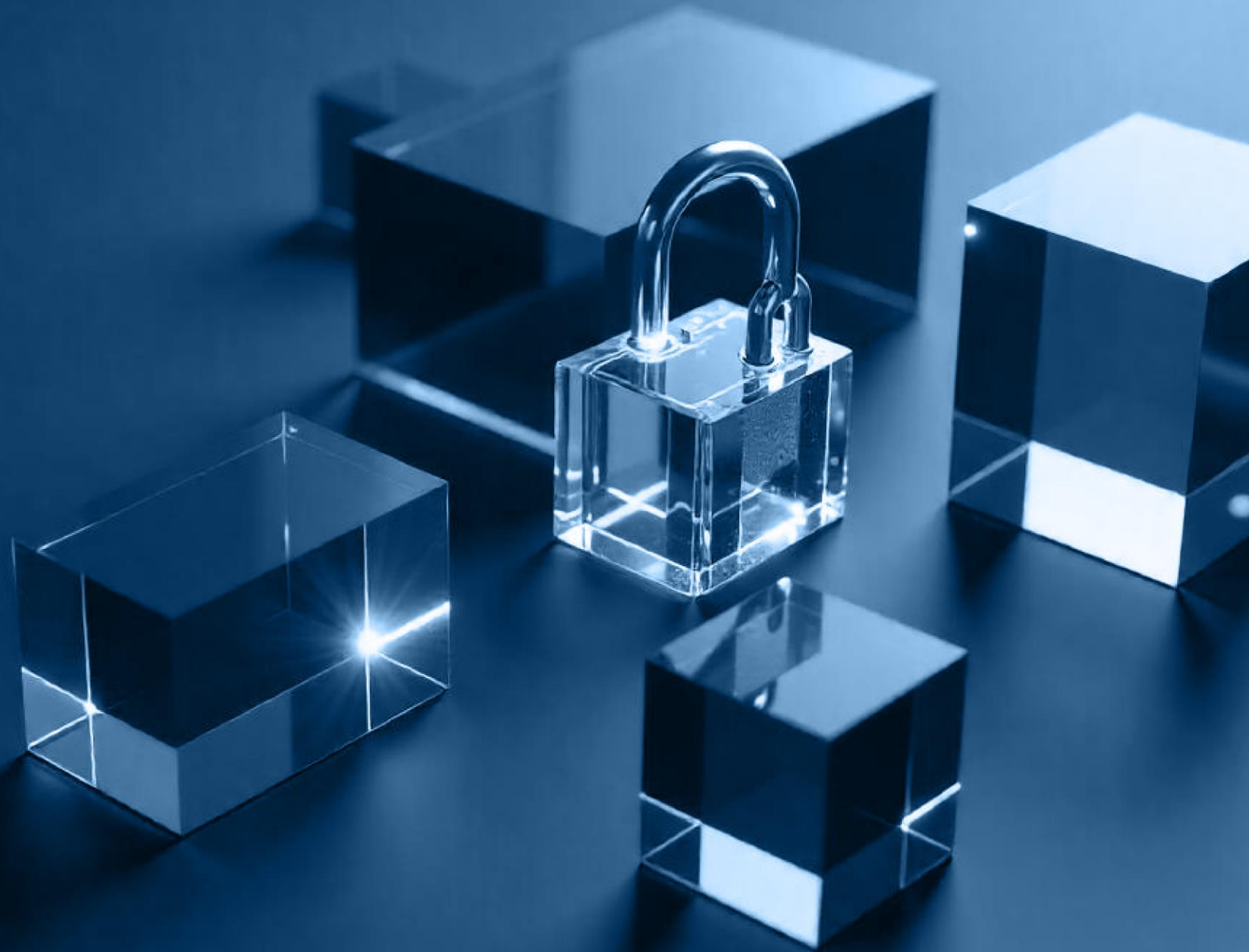
SecretTechnologies



Описание модулей Secret Cloud DRM

О компании Secret Technologies

SecretTechnologies

семейство продуктов*

Secret Cloud

безопасный файловый обмен с сотрудниками и партнерами. SCE сертифицирован ФСТЭК РФ по 4 уровню доверия

DataMask

обезличивание чувствительных данных

с 2016 года

на рынке ИБ

Trace Doc

создание уникальных копий документов

VideoAnalyzer

система автоматизированного анализа видео- и аудиоархивов

> 100 тысяч

пользователей продуктов

Screen Guard

защита экрана монитора от фотографирования

Printer Guard

контроль и экономия печати

8 продуктов

в собственном портфеле решений

*В семейство продуктов Secret Cloud входят: Secret Cloud, Secret Cloud Enterprise, Secret Cloud DRM

Secret Cloud DRM / Модули дополнения

SecretTechnologies

- Мандатное управление доступом
- Классификатор
- Скрытое маркирование

- Коннектор SIEM
- Коннектор Microsoft Exchange
- Коннектор DLP
- Брендирование

Мандатное управление доступом

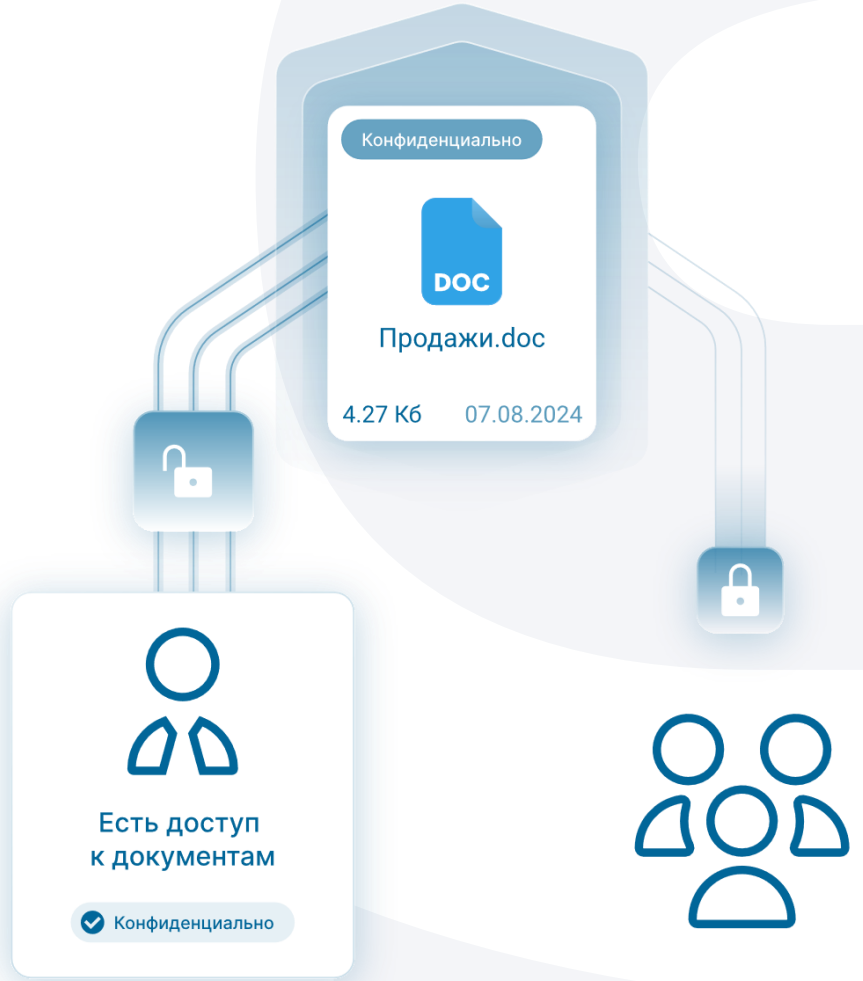
SecretTechnologies

Для чего

Разграничить права доступа с помощью назначения меток безопасности файлам, пользователям и группам пользователей.

Возможности

Позволяет пользователям работать только с теми документами, которые соответствуют их должностным обязанностям.



Мандатное управление доступом / Работа модуля

SecretTechnologies

Пользователь может работать с документом только, если его метка безопасности совпадает с меткой безопасности документа.

Пользователь может запросить изменение метки у администратора.

Мандатное управление доступом / Сценарии использования

SecretTechnologies

Проблема

Модели доступа, принятые в компании, не позволяют фактически разделять доступ к данным, он может быть предоставлен тем, у кого такого доступа быть не должно.

Последствия

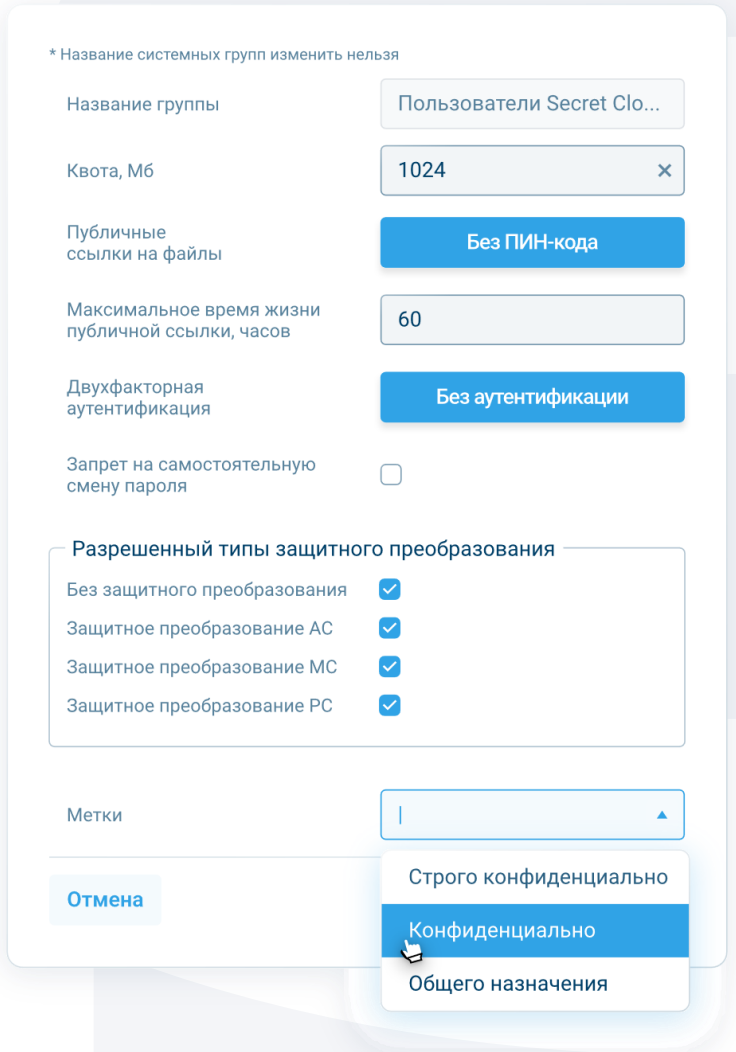
Утечка информации из-за неконтролируемого обмена файлами между сотрудниками.

Решение

Назначение меток безопасности на файлы и пользователей.

Выгода

Исключена вероятность получения доступа к файлам сотрудниками, которым данный доступ запрещен



Классификатор

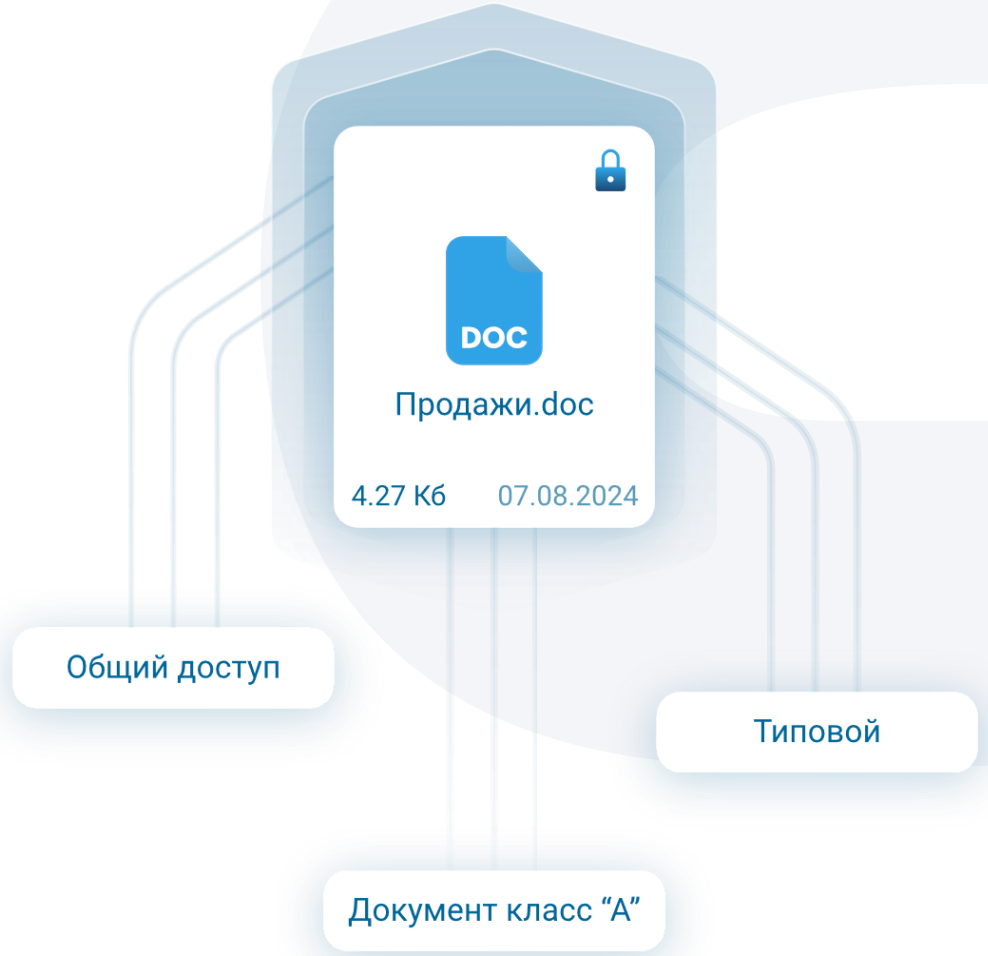
SecretTechnologies

Для чего

Позволяет минимизировать ошибки ручной классификации конфиденциальной информации и экономить время сотрудников при назначении меток безопасности.

Возможности

Автоматическое назначение меток на файлы, путём анализа содержащихся в них данных.

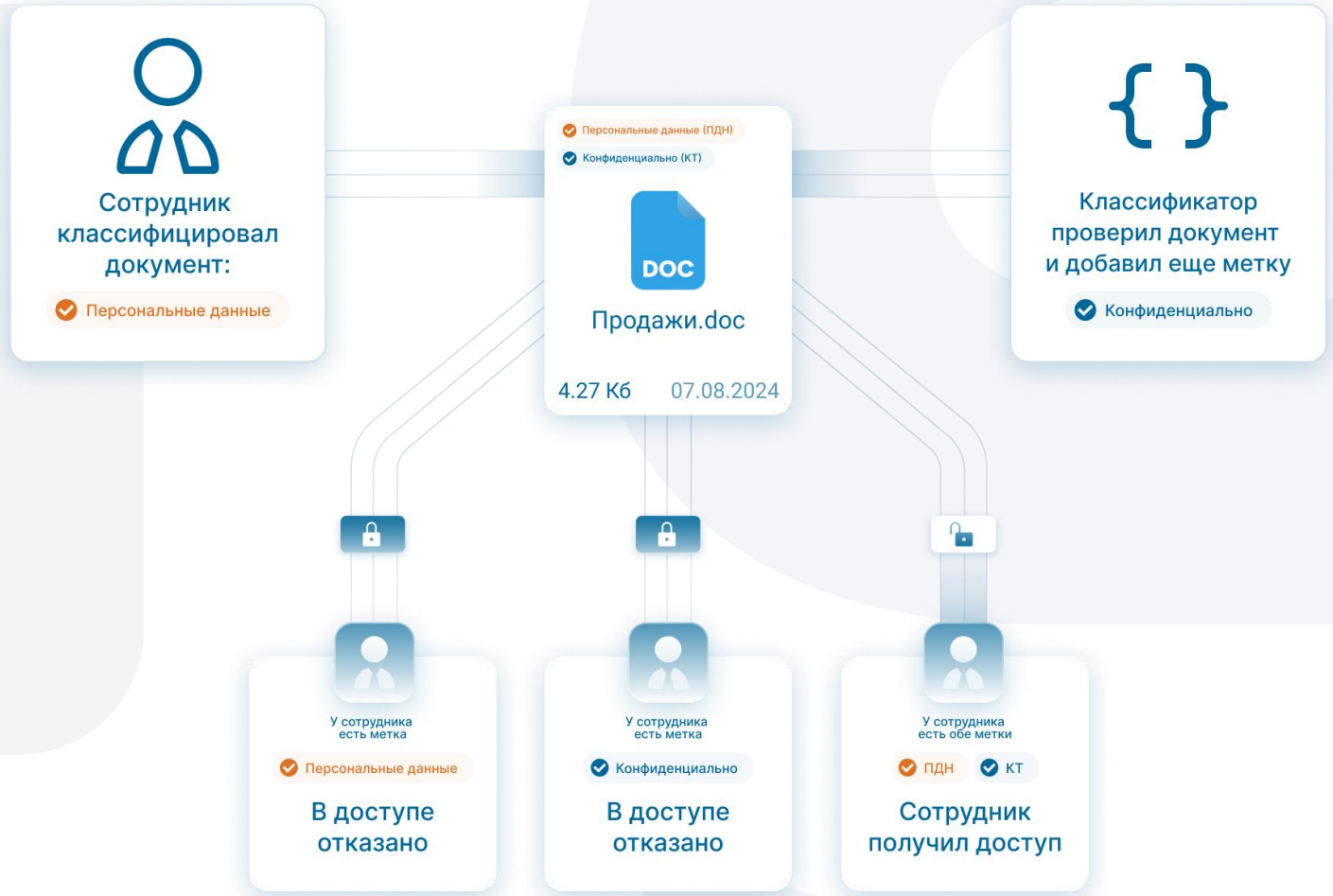


Классификатор / Работа модуля

SecretTechnologies

Система анализирует текст в файле
на основании заданных правил и назначает
метки к файлам в принудительном или
рекомендательном режиме.

Через запрос администратора,
у пользователя будет возможность
изменять метки или наборы меток.



Классификатор / Сценарии использования

SecretTechnologies

Проблема

Сотрудники не всегда корректно определяют конфиденциальность документов или намеренно меняют уровень доступа к информации, что может привести к утечкам данных.

Последствия

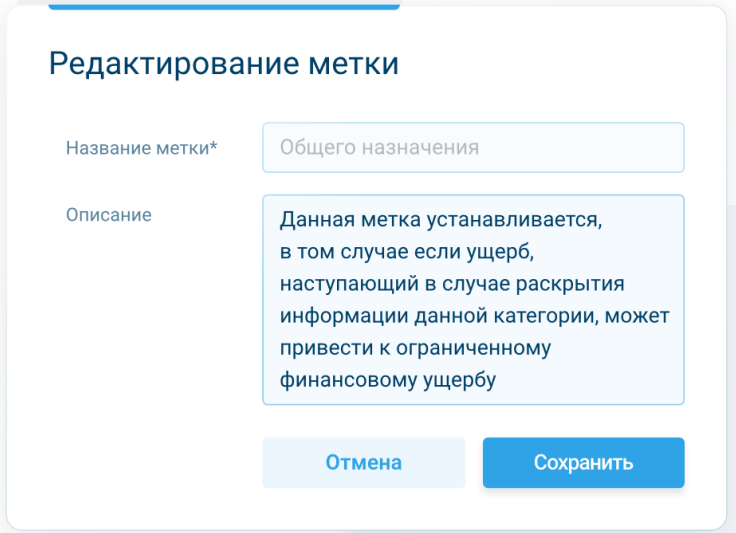
Риск разглашения конфиденциальной информации из-за отсутствия нужной метки.

Решение

Автоматическое проставление меток на файлы без участия сотрудников.

Выгода

Распространение конфиденциальной информации ограничено кругом сотрудников, имеющих право на работу с ней.



Управление цифровыми правами

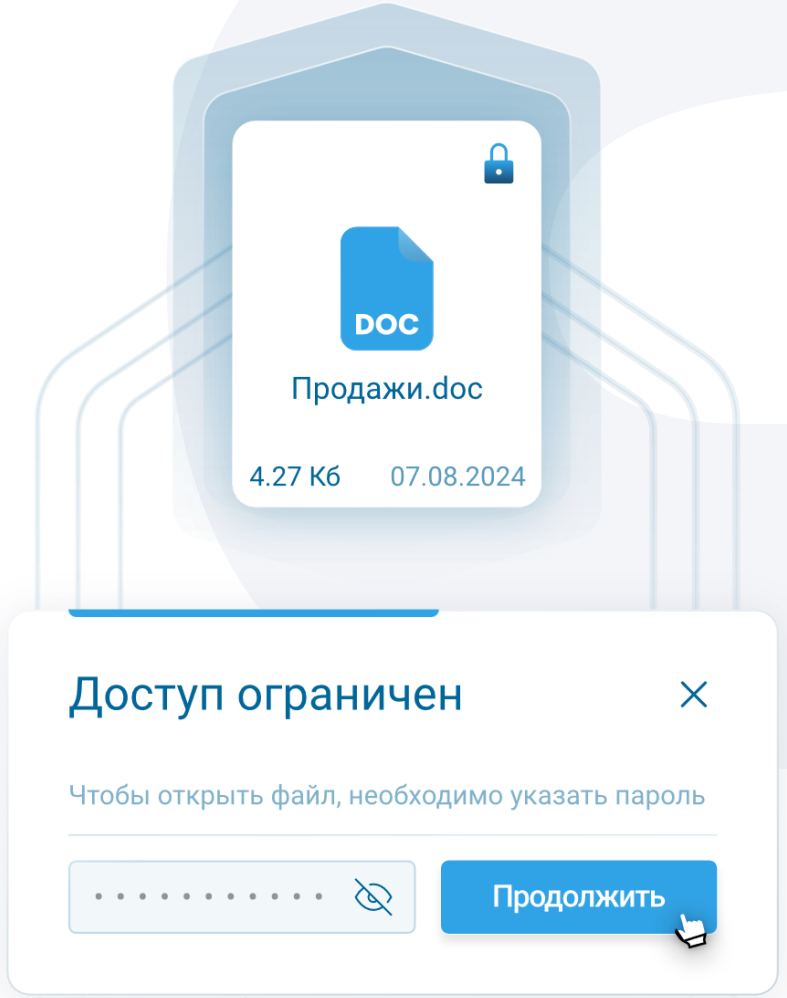
SecretTechnologies

Для чего

Позволяет защитить конфиденциальную информацию от несанкционированного доступа третьими лицами.

Возможности

Размещение файлов в защищённые контейнеры, обеспечивающие дополнительную безопасность.



Управление цифровыми правами / Работа модуля

SecretTechnologies

Создание виртуального диска под конкретного для адресата, где доступ формируется на определенное количество открытий и в течение определенного срока.

Открыть файл можно только на ПК, на котором он был открыт впервые. Работа с файлом ведется в контейнере и извлечь файл из него не получится.

Можно задать типы шифрования (ГОСТ, AES) для сотрудников и контрагентов.

Управление цифровыми правами / Сценарии использования

SecretTechnologies

Проблема

В процессе обмена коммерческой информацией с контрагентами, есть риск передачи данных третьим лицам.

Последствия

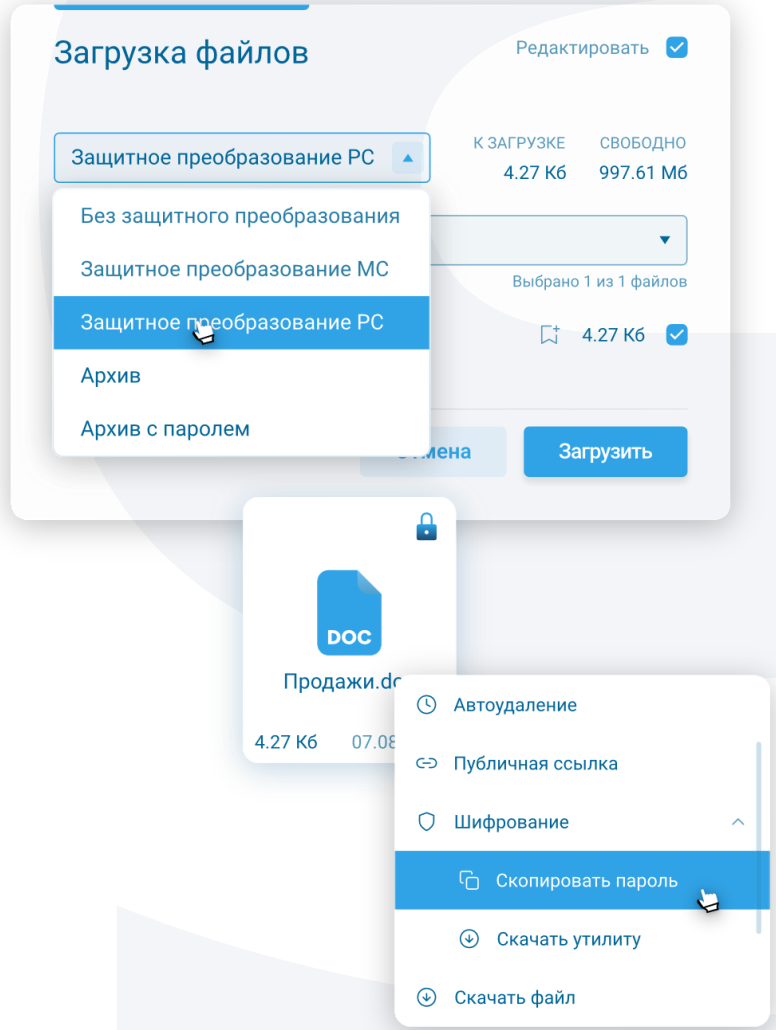
Риски утечки коммерческой информации.

Решение

Контейнеризация файлов для обеспечения дополнительной защиты.

Выгода

Исключена вероятность получения доступа 3-х лиц к конфиденциальным данным.



Управление цифровыми правами / Сценарии использования

SecretTechnologies

Проблема

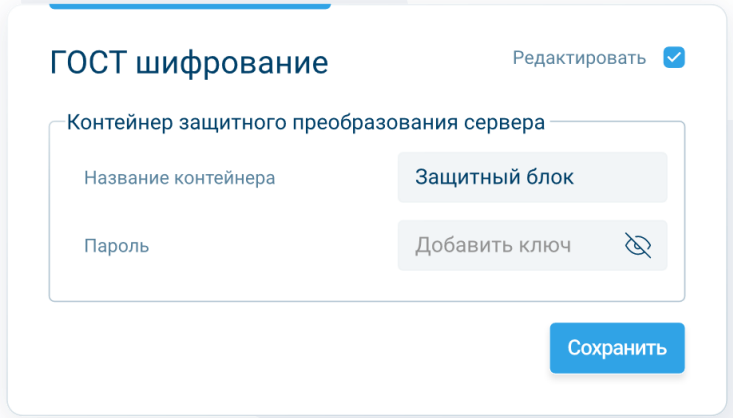
Файлы хранятся в открытом виде на сервере

Последствия

Администратор файлового сервера, имеющий физический доступ к нему, может скопировать файлы

Решение

Преобразование файлов с использованием определенного алгоритма шифрования



Выгода

Файлы зашифрованы, исключена вероятность утечки данных.

Скрытое маркирование

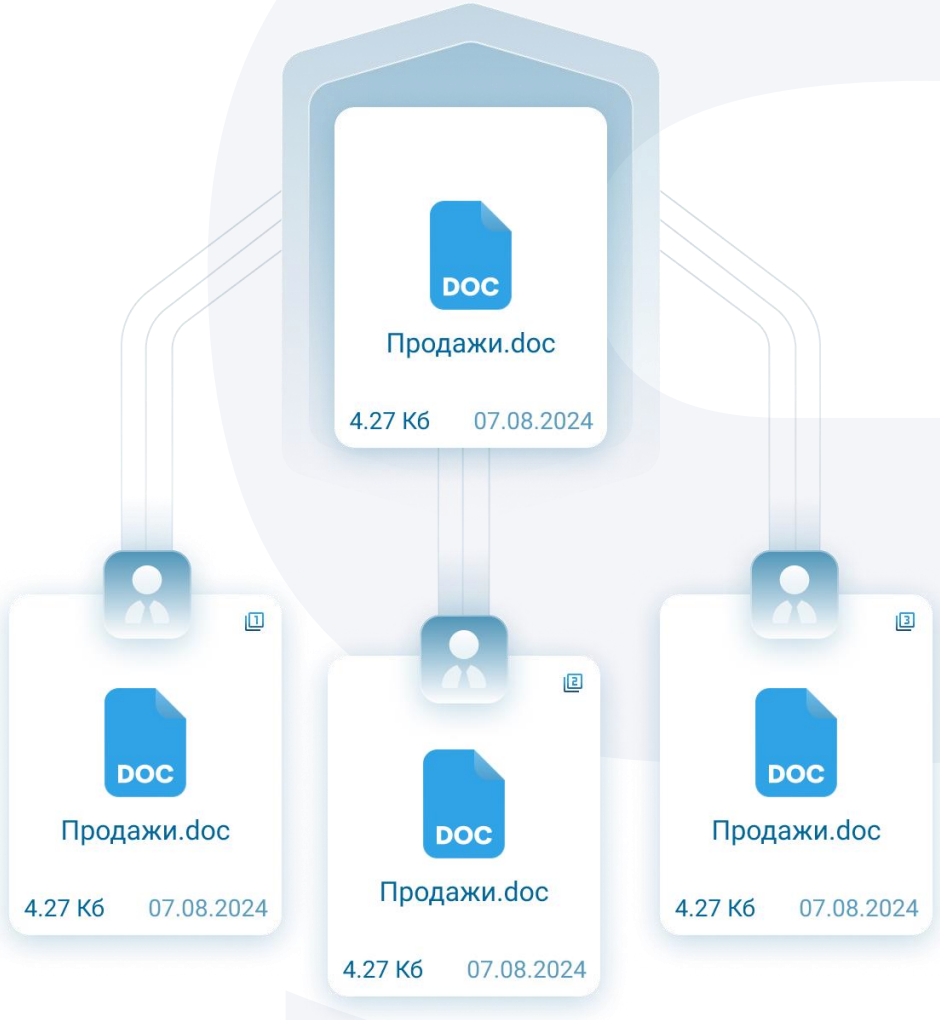
SecretTechnologies

Для чего

Позволяет идентифицировать злоумышленника, разгласившего конфиденциальную информацию через фото или скриншот.

Возможности

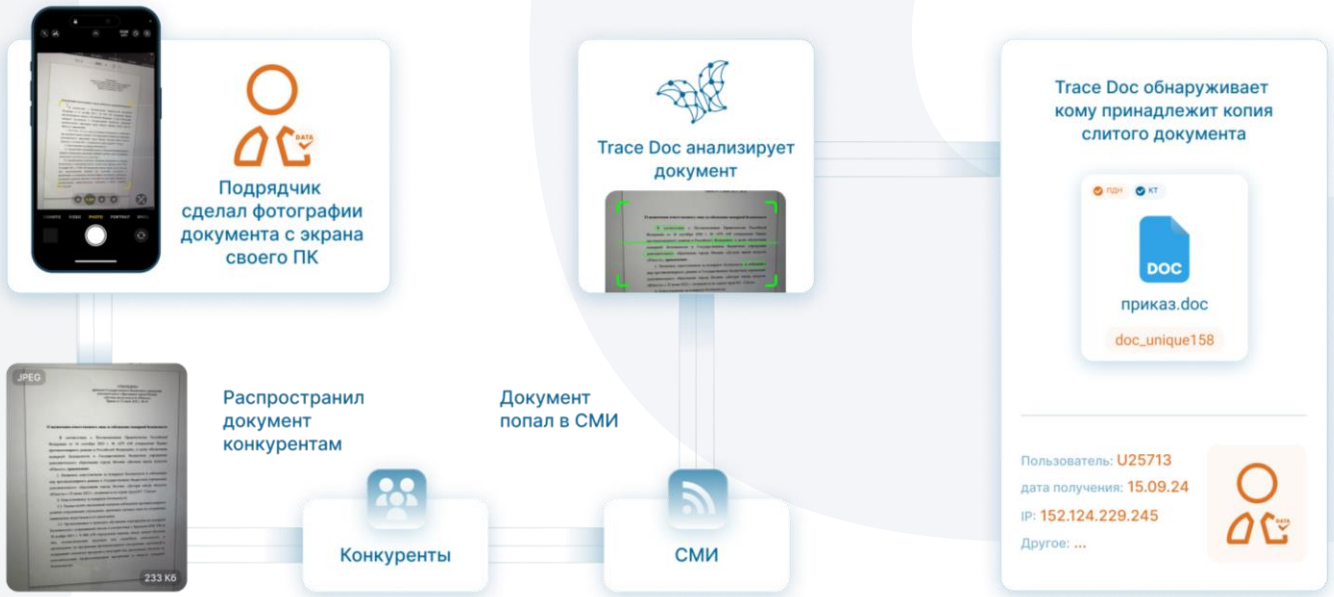
Автоматическое создание уникальных копий документов для каждого пользователя, открывшего файл. Работа с типами данными: скриншоты, фото экрана и распечатанные документы



Скрытое маркирование / Работа модуля

SecretTechnologies

В ходе работы модуля происходит незаметное смещение текста в копии документа, который открывает пользователь для работы.
Таким образом для каждого пользователя появляется уникализированная копия документа.



Скрытое маркирование / Сценарий использования

SecretTechnologies

Проблема

Сотрудник регулярно отправлял конкурентам финансовую информацию по компании, делая снимки экрана.
В компании не могут выявить злоумышленника и канал утечки данных.

Под угрозой

Любая компания, у которой есть конфиденциальная информация и документы, не подлежащие огласке

Решение

Создание уникальных копий документов для каждого пользователя