



SafeCopy

РЕШЕНИЕ ДЛЯ ЗАЩИТЫ ПЕЧАТНЫХ,
ГРАФИЧЕСКИХ И ЭЛЕКТРОННЫХ
КОПИЙ ДОКУМЕНТОВ



КОНФИДЕНЦИАЛЬНО

С развитием информационных систем, защита от потери или несанкционированного распространения конфиденциальных документов, произошедших по вине сотрудников организаций (инсайдеров) или внешних злоумышленников, имеет ключевое значение для любой крупной организации.

➔ ЛУЧШАЯ ЗАЩИТА ОТ ЗЛОУМЫШЛЕННИКОВ – ЭТО SAFECOPY

Решение SafeCopy позволяет предотвратить распространение печатных и электронных копий конфиденциальных документов, несанкционированную передачу их конкурентам компании, представителям прессы, контрагентам и заказчикам. Каждое ответственное лицо в компании, имеющее доступ к печатным и электронным копиям конфиденциальных корпоративных документов, будет иметь возможность работать только со своей уникальной копией, распространение которой приведет к наиболее вероятному определению источника утечки документа.

Знание о работе решения SafeCopy внутри компании удержит сотрудников от необдуманного шага несанкционированного распространения своей печатной или электронной копии, и как следствие, избавит организацию от неприятных ситуаций, скандальных разоблачений, связанных с раскрытием информации, содержащейся в печатных копиях документов.

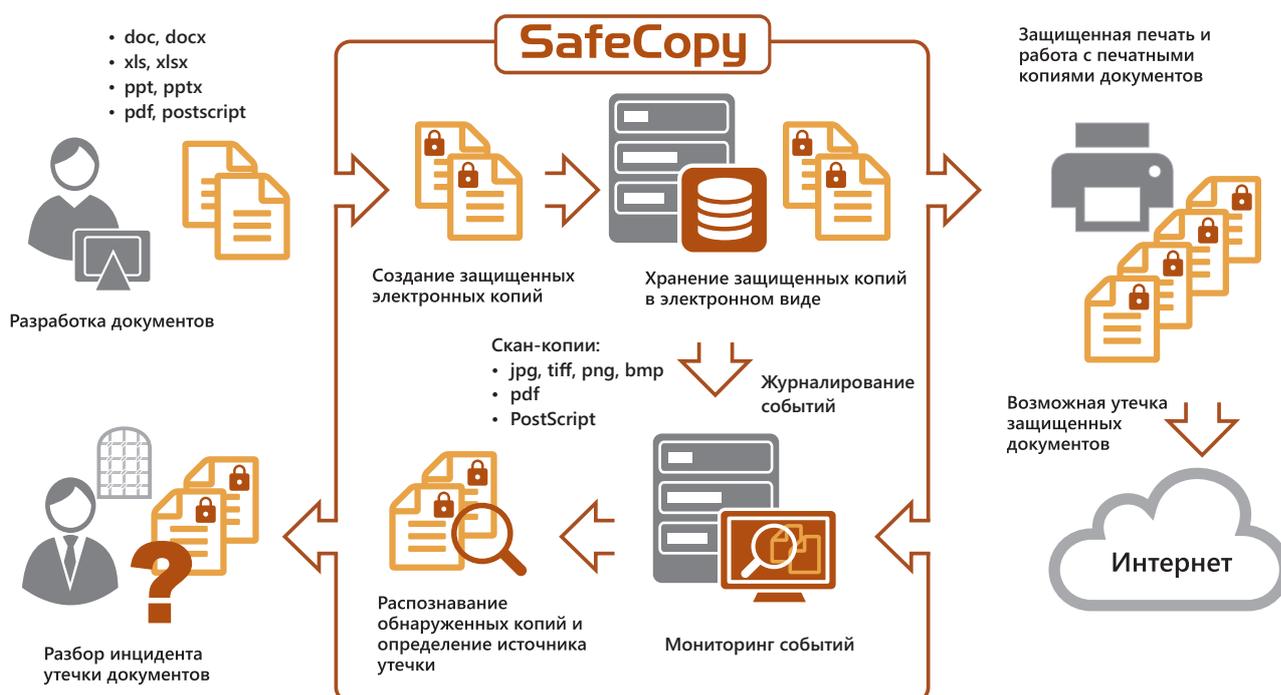
➔ SAFECOPY РЕШАЕТ СЛЕДУЮЩИЕ ЗАДАЧИ:

- выявление каналов утечки печатных копий корпоративных документов и определение нелояльных сотрудников, допустивших несанкционированное распространение документов вовне;
- централизованное хранение, учет и управление документооборотом служебных корпоративных документов, не подлежащих распространению;
- реализация необходимых технических мер, в сочетании с которыми организационные мероприятия и политики информационной безопасности компании позволят провести эффективное расследование любых инцидентов, связанных с несанкционированным распространением печатных копий документов.

➔ ЭФФЕКТ ОТ ИСПОЛЬЗОВАНИЯ СИСТЕМЫ SAFECOPY

- Ограничение бесконтрольного распространения печатных копий защищаемых документов путем создания скрытых маркировок печатных копий и выявления лиц, организовавших утечку конфиденциальной информации.
- Централизованный контроль за распространением печатных и электронных копий конфиденциальных документов.
- Оперативное выявление злоумышленника в случае возникновения инцидента ИБ (канала утечки копии документа).
- Контроль над распространением конфиденциальных документов.

➔ ПРИНЦИП РАБОТЫ



→ КОМПОНЕНТЫ РЕШЕНИЯ SAFECOPY:

- операционная Система: Windows/Linux.
- база данных - PostgreSQL;
- сервер веб-приложений - Apache Tomcat;
- в качестве клиента используется веб-браузер.



→ ТЕХНОЛОГИЯ ЗАЩИТЫ МАРКИРОВКОЙ

Для защиты документов от копирования, незаконного распространения и сохранения авторских прав используется технология защиты маркированием.

ВИДИМАЯ МАРКИРОВКА

- Регистрационный номер документа;
- QR код;
- Иные графические элементы.

Видимая маркировка включает специальные метки, внедряемые в содержимое документа в целях контроля его правомерного использования. Поскольку видимые знаки довольно легко удалить или заменить с помощью графических или текстовых редакторов также применяется скрытая маркировка.

СКРЫТАЯ МАРКИРОВКА

Необходимо контролировать не только цифровое распространение документов, но и печать их бумажных копий. В этом случае для различных пользователей (групп пользователей) можно создавать копии оригинального документа, защищенные скрытой маркировкой. Технология такой защиты построена на внесении в оригинальный документ незначительных, слабо заметных для конечного пользователя изменений (смещение блоков текста, растяжение/сжатие, внесение незаметных артефактов и т.д.). Таким образом, напечатанные разными пользователями документы будут минимально отличаться друг от друга (и от оригинала-шаблона), но при возникновении инцидента ИБ-система дает возможность определить, чья именно печатная копия была скопрометирована.

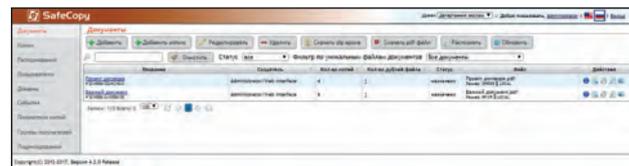
После создания необходимого количества копий в базе данных для каждой копии документа хранится информация о внесенных изменениях (контекст преобразования). Таким образом в базе данных хранятся оригиналы документов и контексты преобразований, сами защищенные копии не хранятся, а создаются «на лету». Для печати всего набора защищенных копий документа генерируется файл, содержащий все защищенные копии выбранного документа, а также листы-разделители, отображающие принадлежность каждой копии конкретному человеку для последующей выдачи копии на руки. Таким образом, процесс печати всех созданных копий является удобным и понятным для сотрудника ответственного за делопроизводство и распространяющего защищенные копии.

РАССЛЕДОВАНИЕ ИНЦИДЕНТА

В случае обнаружения факта несанкционированного распространения защищенной копии документа, сформированной с использованием Системы, предусмотрена возможность проведения расследования инцидента. В результате распознавания печатной копии Система предоставляет выраженную в процентном соотношении степень соответствия найденного документа и подготовленных ранее печатных копий. Если выдача печатных копий, подготовленных к защите, сопровождалась регистрацией получателя и соответствующей маркировкой, то результат распознавания будет содержать достаточные сведения об источнике утечки информации.

→ ПОДДЕРЖИВАЕМЫЕ ФОРМАТЫ ДОКУМЕНТОВ

- Документы, сформированные с помощью Microsoft Office: Word, Excel, PowerPoint. Форматы: doc, docx, xls, xlsx, ppt, pptx. (Для формирования защищенной копии необходимо, чтобы каждая защищаемая страница документа содержала не менее 9 строк текста, при этом допускается любое количество графических элементов таких как картинки, таблицы или иное. Графические элементы (в том числе таблицы) не модифицируются, модификации подвергается только текст (в том числе содержимое таблиц).
- Документы формата PDF (включая различные подмножества такие как PDF/A, PDF/X, PDF/A-1b и другие). Допускается загрузка как PDF в редактируемом формате, так и отсканированные образы документов.
- Файлы postscript (файлы, подготавливаемые драйверами большинства принтеров в процессе предпечатной подготовки).



→ ИНТЕГРАЦИЯ SAFECOPY С ДРУГИМИ КОРПОРАТИВНЫМИ СИСТЕМАМИ

Сервисы SafeCopy могут быть использованы для интеграции с различными внешними Системами, такими как:

- Системы Электронного документооборота (СЭД).
- DLP Системы.
- Системы контроля печати.

Принцип интеграции SafeCopy с системами документооборота един: при внедрении определяются признаки документа в рамках СЭД (согласованный документ, скан-копия и т.д.), по которым СЭД выбирает какую копию необходимо отдавать пользователю – копию без внесенной защитной маркировки или защищенную копию. В случае, если признак установлен, СЭД перехватывает запрос на выдачу файла и вместо хранящегося в нем документа, делает запрос к серверу SafeCopy на создание защищенной копии. SafeCopy на основе информации о пользователе применяет к документу шаблон маркировки и возвращает СЭД защищенную копию. СЭД передает пользователю вместо запрашиваемого файла его защищенное PDF-представление. Вся процедура подмены копии документа остается скрытой от конечного пользователя.

→ ИНТЕГРАЦИЯ SAFECOPY С ПРИЛОЖЕНИЯМИ MICROSOFT OFFICE

Для обеспечения возможности защиты документов, подготовленных с помощью офисных приложений Microsoft, разработан коннектор в виде специализированного встраиваемого плагина для пакета Microsoft Office версий 2007 и выше. Использование этого коннектора обеспечивает возможность инициировать подготовку необходимых защищенных копий корпоративных документов прямо в интерфейсе офисных приложений: Word, Excel, PowerPoint. При этом реализована возможность формирования группы получателей защищенных копий в соответствии с организационно-штатной структурой компании.

В настоящее время разработаны коннекторы SafeCopy к следующим системам электронного документооборота:



СЭД ДЕЛО компании ЭОС;



Docsvision – решение, обеспечивающее все для организации делопроизводства – от упрощенного до полнофункционального, по стандартам и методикам Росархива;



SafeDoc – российское решение для защищенного документооборота.

→ УПРАВЛЕНИЕ ПОЛЬЗОВАТЕЛЯМИ СИСТЕМЫ

В целях разграничения доступа пользователей к функционалу Системы используются следующие механизмы:

- Ролевая модель. Каждому пользователю может быть назначена одна или несколько ролей предусмотренных Системой.
- Разграничение доступа на основе специальных выделенных областей – доменов SafeCopy.
- Пользователи могут быть импортированы из существующего службы каталогов (AD). При этом на основе групп пользователей в AD автоматически может быть применена ролевая модель SafeCopy.
- Доступ пользователя к Системе по логину/паролю, либо с использованием SSO (Single Sign-On) на основе доменной авторизации.

Продукт имеет сертификат соответствия требованиям безопасности информации ФСТЭК России (№2823, выдан ФСТЭК России 22 января 2013г., продлен 22 января 2016)

