Cross Technologies

DOCS SECURITY SUITE

Crosstech Docs security suite (DSS) – это платформа управления, контроля и аудита прав доступа к электронным документам на основе меток конфиденциальности.

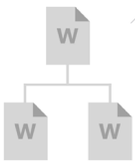
DSS принудительно проставляет визуальные и/или скрытые метки на документы, регистрирует все действия пользователя с документом, прослеживает взаимосвязь документов, разграничивает и контролирует права доступа пользователей на основе матрицы доступа меток конфиденциальности. Вся история событий сохраняется в специализированной базе данных для дальнейшего анализа и расследования инцидентов.

DSS ПОЗВОЛЯЕТ:

– установить визуальную и скрытую метку документу;

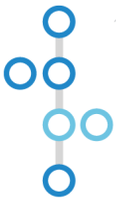
– по запросу пользователя анализировать документ по ключевым словам и выбрать наиболее подходящую метку;

– разграничить доступ пользователей к электронным документам и меткам в соответствии с действующими в организации регламентами и политиками ИБ;



– учесть все обрабатываемые в компании электронные документы и классифицировать их в соответствии с действующими в организации регламентами, политиками ИБ и перечнем сведений, относящихся к информации ограниченного доступа, коммерческой тайне или другому виду тайны;

– учесть всех пользователей, работающих с электронными документами;



– воссоздать и систематизировать всю историю создания документа вне зависимости от существующих в компании систем документооборота: восстановить цепочку создания версий, копий, черновиков документа с чистого листа и до его финальной версии, в том числе все отправки на печать;

– по каждому документу определить его местонахождение, а также кто, где и когда с ним работал;

– фиксировать все действия пользователя при работе с документом;

– оперативно выявить попытки и факты нарушения установленного режима защиты информации и политик информационной безопасности в рамках конфиденциального электронного документооборота,

– по каждому пользователю найти документы, к которым у него есть доступ, узнать где, когда и с какими из них он работал;

– выявить местонахождение всех созданных черновиков и копий в рамках одного документа;

– сократить избыточное копирование документа и выявить неактуальные версии документов, а также облегчить документооборот в компании;

– определить принадлежность к компании документов, найденных за пределами организации (во внешних сетях связи, интернете, на съемных носителях).

СФЕРЫ ПРИМЕНЕНИЯ – РЕШАЕМЫЕ ЗАДАЧИ

1

РЕАЛИЗАЦИЯ ПРИНЯТОГО В ОРГАНИЗАЦИИ РЕЖИМА ЗАЩИТЫ ИНФОРМАЦИИ

Для любой политики ИБ или режима защиты информации ограниченного доступа (коммерческой тайны, персональных данных, государственной тайны или иного режима) помимо внедрения традиционных процедур и организационно-распорядительных документов необходимо:

а) Внедрение процесса маркирования электронных документов

Проставление визуальной и цифровой метки с заданным уровнем конфиденциальности информации при создании и редактировании электронного документа в соответствии с внедренным в организации перечнем сведений, относящихся к информации ограниченного доступа и/или коммерческой тайне или другому виду тайны. Этот процесс должен быть автоматизирован и максимально прост для пользователя, а также обязателен при работе со всеми электронными документами.

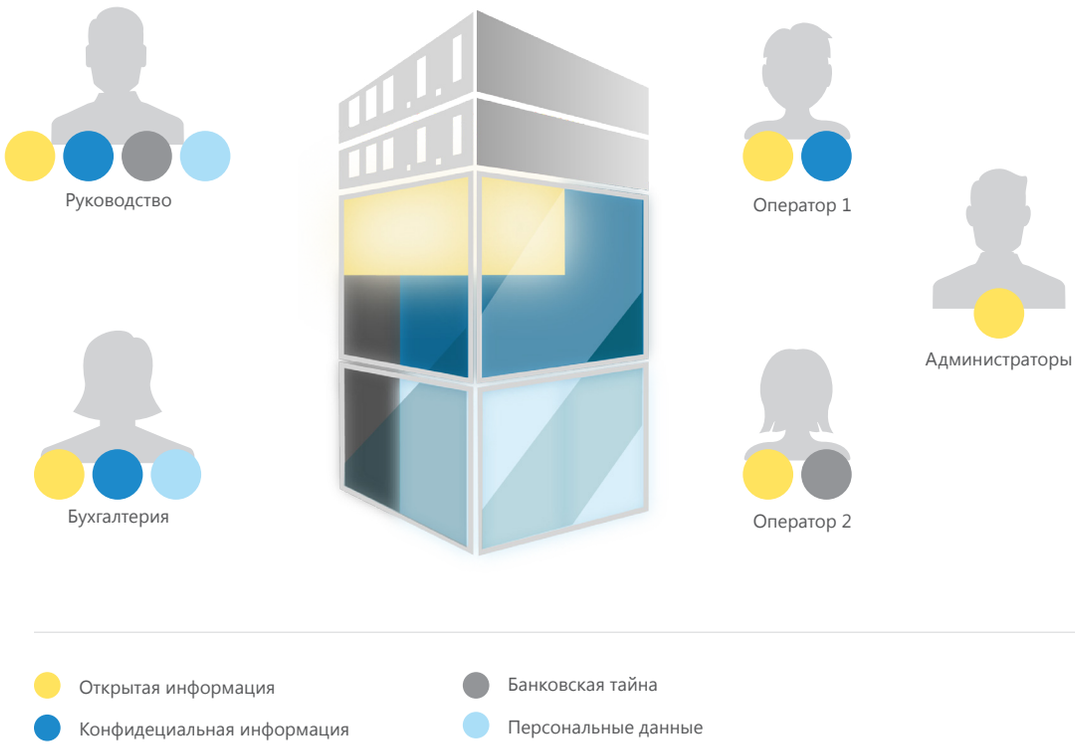
б) Разграничение доступа пользователей к электронным документам

Сегодня существует много вариантов разграничения доступа пользователей к информации. Это могут быть встроенные механизмы защиты ОС, БД, приложений, а также различные сертифицированные ФСТЭК наложенные средства защиты информации (электронные замки и/или программные средства).

Но как показывает практика создания систем защиты информации, все сводится к формальному соответствию требованиям. Большинство защищает только объект, а именно разграничивает доступ к АРМ, сегменту сети, серверу, папке или конкретному документу. При этом забывают разграничить доступ внутри информационной системы, которая обрабатывает конфиденциальную или критичную информацию.

Известно, что разграничивать доступ к серверу или папке неэффективно, это полумера, а ограничивать доступ к конкретному документу довольно тяжело с точки зрения администрирования и ведения бизнес-процессов (особенно если в организации не одна тысяча человек).

Гораздо эффективнее точечно ограничить доступ, т. е. некоторому набору ролей предоставить доступ к разному набору меток (открытая, конфиденциальная, коммерческая тайна, банковская тайна, персональные данные, государственная тайна (секретно, совершенно секретно) и т.п.).



в) Ведение журнала электронной безопасности

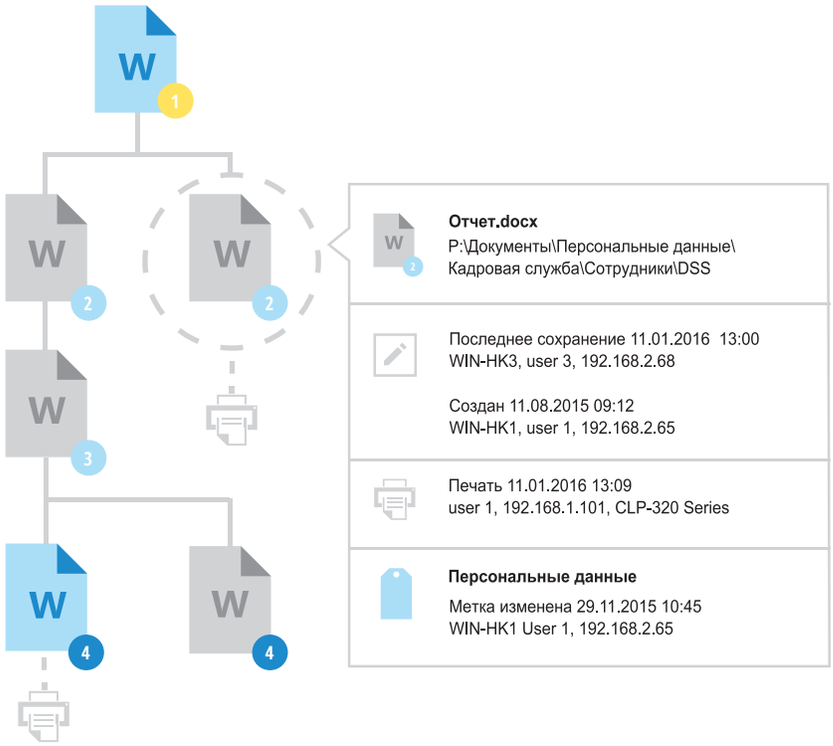
Запись в БД всех выбранных событий регистрации. Регистрация всех действий пользователей: создание, изменение, копирование, печать документа, автор, пользователи, дата, время, и прочие данные при работе с документами.

г) Ведение автоматизированной аналитики

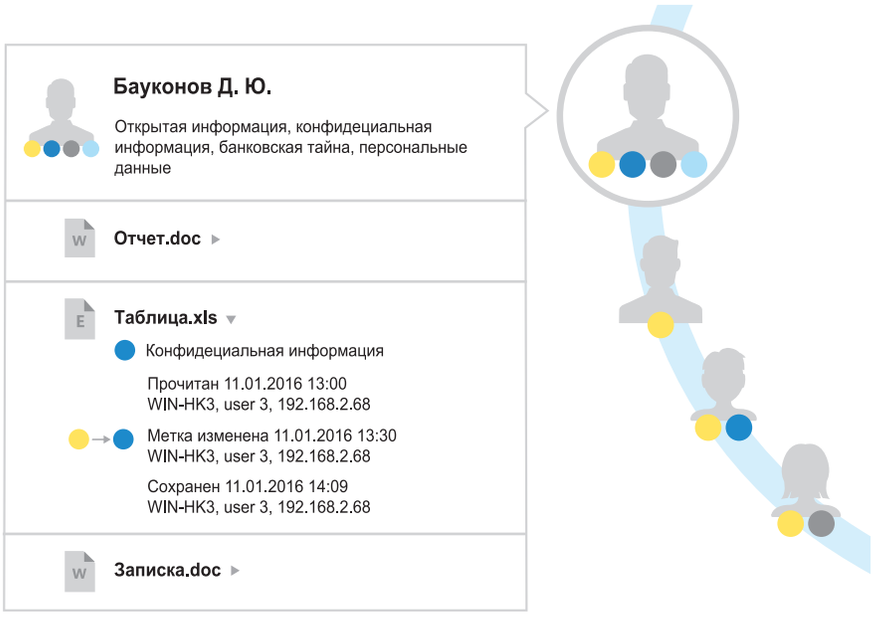
Ведение автоматизированной аналитики при выборе тех или иных фильтров DSS позволяет:

- определить местонахождение документа, а также кто и когда с ним работал;
- воссоздать и систематизировать всю историю электронного документа, включая восстановление цепочки создания версий, копий, черновиков документа с чистого листа и до его финальной версии, в том числе все отправки на печать;

– выявить местонахождение всех созданных черновиков и копий в рамках одного документа;



– определить где, когда и с какими документами работал пользователь (локально и/или на сетевых ресурсах), какой доступ имеет;



- определить принадлежность к компании документов, найденных за пределами организации (во внешних сетях связи, интернете, на съемных носителях);
- предоставить актуальную и детальную информацию для расследования инцидентов;
- оперативно выявить попытки и факты нарушения установленного режима защиты (политик ИБ): например, если кто-то из пользователей пытался несанкционированно изменить документ, скопировать конфиденциальный текст в документ с отличным типом метки или в почтовый клиент, удалить метку и/или свойства документа;
- облегчить документооборот в компании.

д) Внедрение классификации электронных документов

Классификатор анализирует документ по ключевым словам, классифицирует его, и автоматически предлагает выбрать пользователю наиболее подходящую метку. Его можно запустить в автоматическом режиме сканирования диска или папки.

2

ВЫПОЛНЕНИЕ ТРЕБОВАНИЙ ФЕДЕРАЛЬНОГО ЗАКОНА № 98-ФЗ “О КОММЕРЧЕСКОЙ ТАЙНЕ” ОТ 29.07.2004 ГОДА

Большинство организаций пребывает в уверенности, что успешно внедрили режим защиты коммерческой тайны, и, зачастую, это является заблуждением.

Важнейшими мероприятиями по внедрению режима защиты коммерческой тайны являются формирование перечня отнесенных к коммерческой тайне сведений и маркирование документов, содержащих коммерческую тайну.

При этом ни одна организация при обмене электронными документами и сообщениями в файлах, таблицах, изображениях, презентациях, электронных письмах, никак их не маркирует, или маркирует все подряд. Тем самым конфиденциальные сведения никак не выделяются из общего потока обрабатываемой информации.

Кроме того, 98-ФЗ «О коммерческой тайне» не содержит понятия электронного документа и сообщения, все внимание сводится к учету и маркированию именно материальных носителей, содержащих информацию, составляющую коммерческую тайну.

Поэтому большинство организаций «забывают» про электронный документооборот и, при внедрении мероприятий п. 1 ст. 10 98-ФЗ, избегают маркирования электронных документов/сообщений, содержащих коммерческую тайну.
Как следствие, организация не знает, где в ее инфраструктуре реально обрабатывается и хранится информация, относящаяся к коммерческой тайне, кто к такой информации имеет или имел доступ.

Тем самым сотрудники и контрагенты компании при работе с электронными документами и сообщениями, содержащими коммерческую тайну, не несут ответственности в случае разглашения данной информации и не обязаны соблюдать режим защиты коммерческой тайны.

Для организации это означает фактическое отсутствие режима защиты коммерческой тайны, тем более, что электронные документы и сообщения зачастую составляют до 99% документооборота.

В целом ситуация с маркированием электронных документов и сообщений может быть экстраполирована на любые типы информации ограниченного доступа, в отношении которых установлены требования конфиденциальности.

Поэтому нельзя говорить о том, что в организации внедрен какой-либо режим защиты, если она не маркирует и не выделяет из общего электронного документооборота документы, содержащие конфиденциальные сведения.

Таким образом, любой введенный режим защиты информации неэффективен без внедрения процесса учета и маркирования всех обрабатываемых электронных документов.

ТЕХНИЧЕСКИЕ ТРЕБОВАНИЯ

DSS предназначен для работы с Microsoft Office (Word, Excel, Visio, PowerPoint).

МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ К РАБОЧИМ СТАНЦИЯМ КЛИЕНТОВ

Microsoft Windows

- XP (с пакетом обновлений SP3 или более поздним для 32-bit версии;
- 7 (32/64-bit);
- 8 (32/64-bit);
- 8.1 (32/64-bit);
- 10 (32/64-bit).

Microsoft Office:

- 2007 32-bit с пакетом обновлений SP3*;
- 2010 32/64-bit*;
- 2013 32/64-bit*;
- 2016 32/64-bit*.

* Для всех версий должна быть явно установлена поддержка расширений .NET Framework 3.5

МИНИМАЛЬНЫЕ ТРЕБОВАНИЯ К СЕРВЕРУ

Microsoft Windows Server:

- 2008 (32/64-bit);
- 2008 R2 (32/64-bit);
- 2012 (64-bit);
- 2012 R2 (32/64-bit);

NET Framework 3.5;

SQL Server:

- 2005;
- 2008;
- 2008 R2;
- 2012;
- 2014.

АППАРАТНОЕ ОБЕСПЕЧЕНИЕ

- Процессор с тактовой частотой от 1 ГГц;
- 1 ГБ оперативной памяти (рекомендуется 2 ГБ);
- От 16 ГБ свободного места на жестком диске.