



CROSSTECH
SOLUTIONS GROUP

Docs Security Suite

Crosstech Solutions Group

Российский разработчик решений для мониторинга, контроля и комплексной защиты от внутренних угроз с учетом специфики каждой отдельной организации.

Продукты входят в реестр российского ПО и рекомендованы для импортозамещения на предприятиях России.

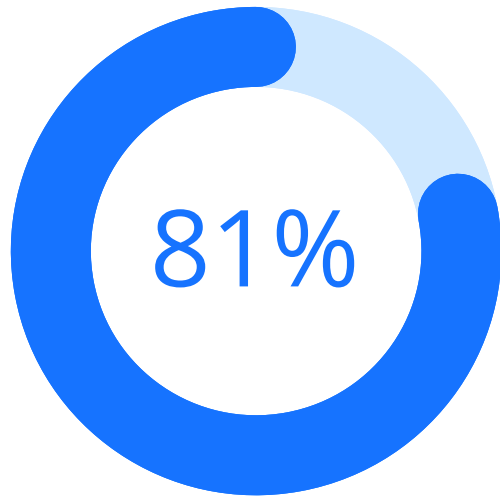


6
решений

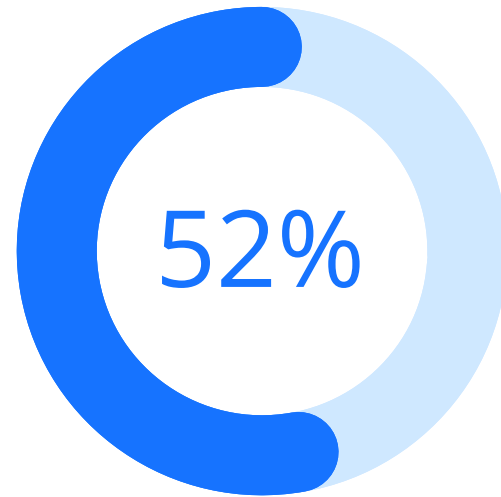
>50
актуальных
партнеров

5
лет на
IT-рынке

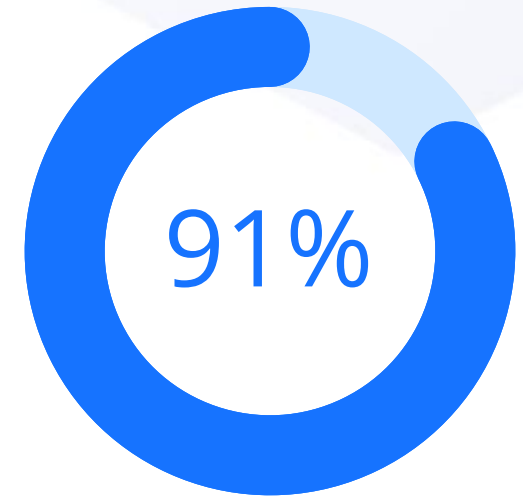
Внутренние угрозы



Утечек в российских компаниях, совершаемых во внутреннем контуре, являются умышленными



Инцидентов происходили по причине «злоупотребления привилегиями» и нарушения прав доступа



Составляет доля утечек персональных данных

Важность защиты

Для ИТ/ИБ директоров

Обеспечение стабильной работы ИТ-инфраструктуры с минимизацией рисков возможной компрометации информации при работе с документами и конфиденциальной информацией

Для офицеров ИБ

Сбалансированная защита конфиденциальности, целостности и доступности данных. Ускорение процесса обнаружения утечки, установления злоумышленника и реагирования на инцидент

Для сотрудников

Повышение ответственности при работе с конфиденциальной информацией, понимание политик информационной безопасности компании

Docs Security Suite (DSS)

Платформа маркирования, уникализации и шифрования электронных документов, позволяющая разграничить доступ пользователей к конфиденциальной информации и настроить политики действий с документами

Jay Data

Российская платформа, осуществляющая поиск, классификацию, маскирование конфиденциальной информации в базе данных, что позволяет компаниям обеспечить надежную защиту чувствительных данных от нелегитимного использования сотрудниками и сторонними лицами

DataNova Object Recognition (OR)

Решение, реализованное на основе глубоких нейронных сетей в алгоритмах компьютерного зрения, позволяющее с помощью перехвата видеопотока с веб-камеры осуществлять мониторинг за деятельностью сотрудников, выявлять нелегитимную активность согласно настроенным политикам безопасности

Решения Crosstech Solutions Group

DataGrain RUMA

Аналитическая платформа, предназначенная для анализа и внутреннего мониторинга действий пользователей и сущностей, построения профилей активности в различных разрезах, выявления аномалий и подозрений на инциденты

DataGrain ESO

Решение, предназначенное для сбора, профилирования, сжатия и хранения событий ИБ, с возможностью разграничения прав доступа и осуществления статистического анализа собираемых данных

CrossTech Smart Assets (CTSA)

Комплексный продукт, ориентированный на физический учёт, финансовый контроль и управление контрактными обязательствами ИТ-активов организации в течение всего жизненного цикла

Docs Security Suite

Docs Security Suite (DSS)

российская платформа маркирования, уникализации и шифрования электронных документов, позволяющая разграничить доступ пользователей к конфиденциальной информации и настроить политики разрешенных действий с документами

Снижение ложных срабатываний
DLP-системы более чем на 80%

DSS включен в единый реестр
российского ПО МИНКОМ связи
№4427 от 16.04.2018

Соответствие требованиям
Регуляторов: 152-ФЗ, 161-ФЗ,
ФСТЭК №17, ГОСТ Р 57580.4-2022

Модули Docs Security Suite

Маркирование

Добавление как скрытых, так и видимых меток конфиденциальности в документе

Логирование

Фиксация всех действий пользователя при работе с документами, даты, времени, атрибутов пользователя и рабочей станции

Разграничение доступа

Получение информации о правах пользователя. Ограничение доступа к документу, если у пользователя нет прав на основе меток конфиденциальности

Шифрование

Использование алгоритмов AES или ГОСТ (КриптоПро CSP) для защиты от несанкционированного доступа и открытия случайным получателем вне контура безопасности

Уникализация

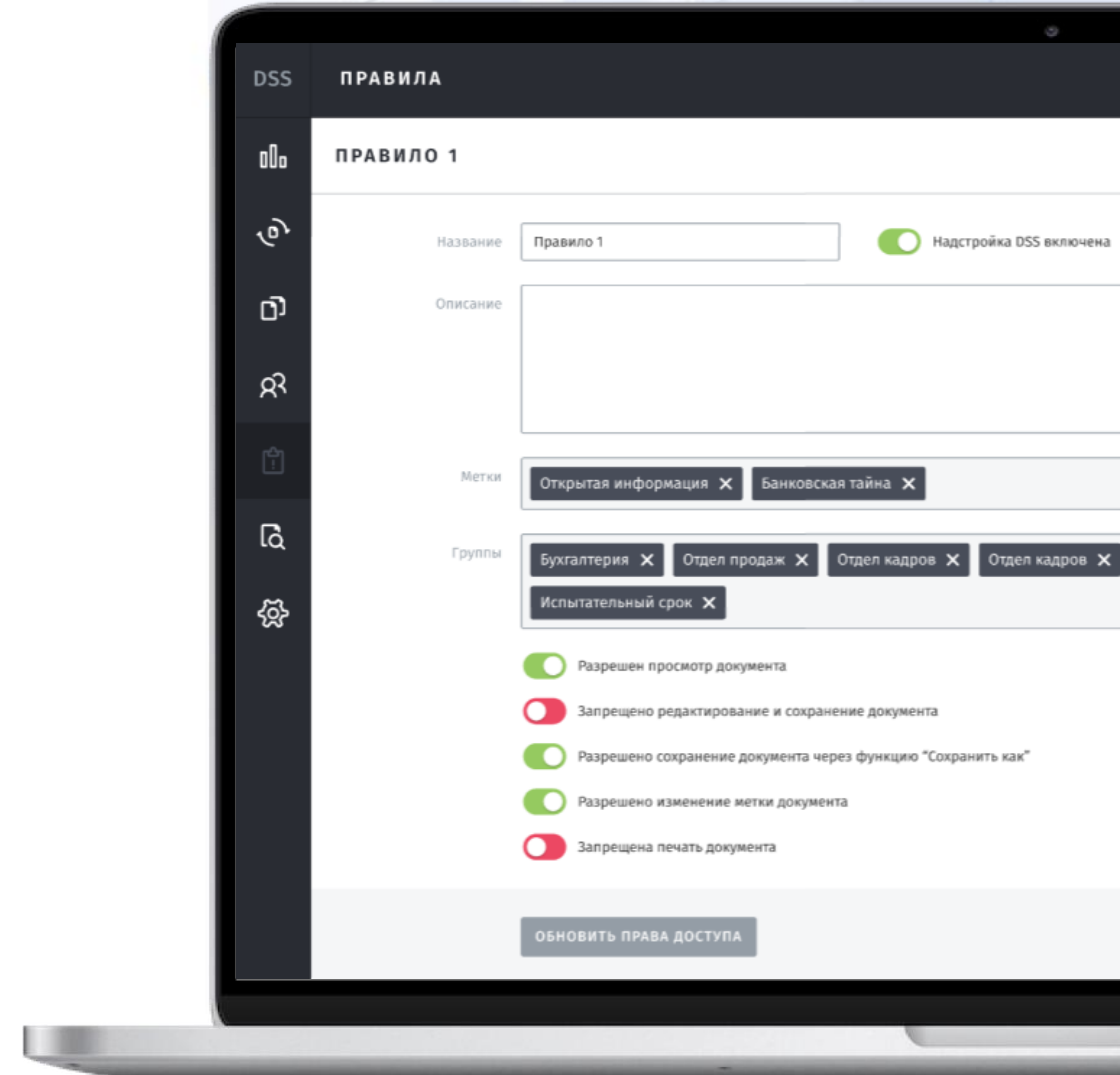
- Уникализация документа на основе технологии стеганографии и аффинных преобразований
- Идентификация принадлежности уникализированного документа по сотруднику

Схема работы Docs Security Suite

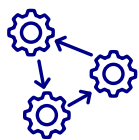


Задачи, решаемые DSS

- **Разграничение доступа**
сотрудников к документам по меткам конфиденциальности
- **Уникализация**
документов с возможностью дальнейшего расследования утечек
- **Шифрование**
критически важных документов компании
- **Фиксация**
фактов нарушения политик безопасности и оповещение ответственных
- **Логирование**
действий сотрудников при работе с документами
- **Осознанный подход**
к обеспечению безопасности информации со стороны сотрудников при работе с документами



Результат внедрения DSS



Выявление нарушителя, сфотографировавшего экран/распечатавшего документ, копия которого утекла, за счет скрытых стегано меток



Централизованная и непрерывная регистрация всех доступов и попыток доступа к документам организации



Гарантированное уничтожение документа, всех его копий и черновиков



Доступ к документу и всем его копиям может быть централизованно изъят вне зависимости от того где они и у кого

Кейс. Случайная утечка информации



Описание ситуации

При отправке конфиденциального документа по электронной почте в адресной строке пользователь случайно указывает однофамильца получателя или иного адресата, находящегося вне контура ИБ

При отсутствии DSS

При отсутствии в организации систем класса DLP, письмо будет доставлено и содержимое документа будет скомпрометировано сторонним лицом. В случае их наличия, отправка письма зависит от контентного анализа и принятия решения со стороны администратора DLP, что тормозит бизнес-процессы

При использовании DSS

DSS позволяет разграничивать права на работу с документами и электронными письмами. В настройках работы с определенными метками конфиденциальности можно запретить отправку писем с определенными метками за контур организации

Кейс. Утечка фото с содержимым документа



Описание ситуации

У сотрудника организации имеется доступ к конфиденциальному документу. Пользователь фотографирует содержимое документа и выносит его за контур ИБ

При отсутствии DSS

В случае, когда у пользователя стоит система решения класса DAG/DCAP, – отследить утечку конфиденциальной информации невозможно.

Заявленная функциональность систем класса DLP зачастую не позволяет выявить нарушителя

При использовании DSS

С помощью уникализации экрана по технологии стеганографии сотрудник службы безопасности за короткий срок может провести расследование и точно определить пользователя, допустившего утечку и его последнюю активность с документом

Кейс. Перемещение документа за контур ИБ



Описание ситуации

Злоумышленник обманом вынудил сотрудника организации вынести и передать документ за пределы защищаемого контура

При отсутствии DSS

В случае использования систем класса DLP или DAG/DCAP можно зафиксировать место утечки документа. При этом содержимое документа все равно будет доступно злоумышленнику

При использовании DSS

DSS позволяет зашифровать документ при помощи AES-шифрования или алгоритма ГОСТ (КриптоПро CSP), таким образом злоумышленник не сможет получить доступ к конфиденциальной информации

Кейс. Похищение содержимого документа



Описание ситуации

Преследуя цель незаконного обогащения сотрудник пытается скопировать и пересохранить содержимое конфиденциального документа в другой файл на ПК для последующей продажи данных

При отсутствии DSS

В случае отсутствия мер по обеспечению безопасности сотрудник скомпрометирует данные компании, что может привести к финансовым и репутационным рискам. Функциональность решений класса DLP не позволяет устанавливать ограничения на копирование содержимого документа и вставку его через буфер обмена в любое другое приложение вне защищаемого контура

При использовании DSS

DSS позволяет контролировать и настраивать роли и права доступа пользователей на основе меток конфиденциальности.

Следовательно, пользователю при разрешенной возможности открывать и просматривать документ можно запретить выполнять следующие действия при работе с документом:

- «сохранить как»;
- «копировать»



CROSSTECH

SOLUTIONS GROUP

При возникновении вопросов,
пожалуйста, обращайтесь

+7 (495) 532 10 96

Москва, Ленинградский пр. 31А, стр. 1

info@ct-sg.ru