

Предотвращение утечки данных и защита электронных документов с помощью InfoWatch Traffic Monitor и Oracle Information Rights Management

Одной из важных задач для современных компаний является централизованная защита конфиденциальных электронных документов и предотвращение утечки корпоративной информации. Для защиты электронных документов (независимо от их формата, места хранения и используемой системы документооборота) от утечек из корпоративной сети, компании Oracle и InfoWatch предлагают интегрированное решение на основе продуктов Oracle Information Rights Management (Oracle IRM) и InfoWatch Traffic Monitor.

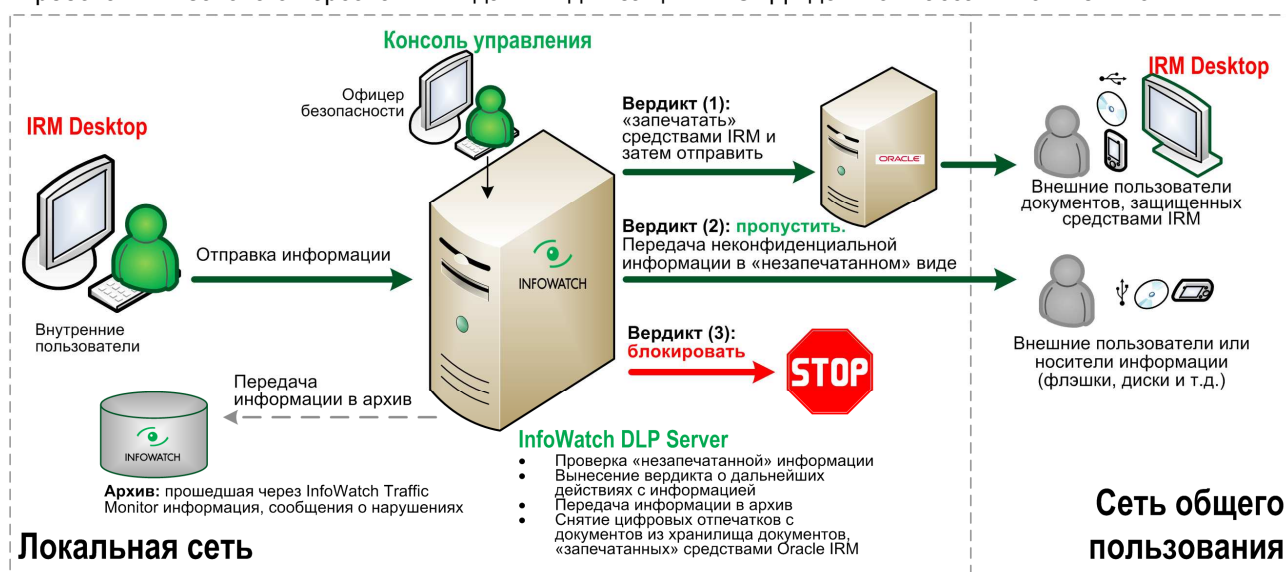
Совместное решение Oracle и InfoWatch обеспечивает централизованный контроль доступа к конфиденциальным электронным документам и отличается простотой и скоростью внедрения. Решение позволяет осуществлять централизованный аудит операций (в том числе вывода на печать) с электронными документами и их централизованное уничтожение в соответствии с действующими корпоративными регламентами и требованиями Законодательства по защите конфиденциальной информации.

Основная функциональность совместного решения:

- Централизованный контроль доступа к конфиденциальным документам на этапе создания, хранения и распространения внутри и за пределами корпоративной сети с помощью технологии «запечатывания»¹.
- Централизованное уничтожение конфиденциальных документов по истечении срока их действия².
- Контроль каналов возможной утечки конфиденциальной информации (web, e-mail, системы мгновенного обмена сообщениями (ICQ и пр.), локальная и сетевая печать, запись информации на съемные носители).
- Блокирование передачи/записи на съемные носители конфиденциальной информации, если это действие нарушает политику информационной безопасности компании.
- Централизованный аудит операций с конфиденциальными документами.
- Централизованное хранение информации об инцидентах утечки данных с возможностью ретроспективного анализа и сбора доказательств для расследования, в том числе судебного согласно Законодательству РФ.

Архитектура решения

Совместное решение включает в себя продукты Oracle IRM и InfoWatch Traffic Monitor, которые сертифицированы ФСТЭК России на соответствие требованиям безопасности информации в АС по классу 1Г и требованиям Закона о персональных данных для защиты ИСПДн до 1-го класса включительно.



¹ Упаковывание информации слоем кодирования, встраивание в кодируемый документ набора ссылок на Oracle IRM Server и добавление цифровой подписи

² По истечении жизненного цикла документа с сервера Oracle IRM удаляется ключ декодирования, без которого невозможно получить доступ к документу

Компоненты решения

Oracle Information Rights Management (IRM)

Oracle IRM – технология информационной безопасности, которая контролирует и защищает информацию везде, где она хранится и используется. Обычные продукты такого класса управляют документами, электронными сообщениями и web-страницами только тогда, когда они хранятся в серверных репозиториях (хранилищах данных). Решение **Oracle** использует кодирование – «запечатывание» – и расширяет возможности по управлению критической для компании информацией, везде, где она хранится и используется: на рабочих станциях пользователей, ноутбуках и мобильных переносных устройствах, в других хранилищах данных, внутри организации и снаружи, за пределами межсетевых экранов (вне корпоративной сети).

Oracle IRM обеспечивает реальный периметр управления документами, электронными сообщениями и web-страницами. При «запечатывании»

- происходит упаковывание информации слоем кодирования, так что, независимо от того, как много копий сделано и где они хранятся, они бесполезны без соответствующих данных для раскодирования;
- в кодируемый документ встраивается набор ссылок (URL links), так что каждая копия ссылается на сервер **Oracle IRM**, на котором информация была «запечатана»;
- используется цифровая подпись, так что любая попытка подделки документов будет определена и предотвращена.

Сами права доступа на «запечатанные» документы хранятся отдельно от данных, на расположенном в сети сервере **Oracle IRM**, который обслуживает организация-собственник документов.

InfoWatch Traffic Monitor

InfoWatch Traffic Monitor – комплексное модульное решение по защите информации от внутренних угроз, которое позволяет контролировать различные каналы утечки данных. Решение включает в себя модуль для защиты рабочих станций, чтобы предотвратить утечку данных через локальную печать, съемные носители информации и коммуникационные порты, модуль для защиты периметра сети, контролирующий корпоративную почту, web, системы обмена сообщениями и сетевую печать, и модуль централизованного хранения и управления.

InfoWatch Traffic Monitor осуществляет:

- Мониторинг и анализ данных, отправляемых за пределы корпоративной сети через почтовые системы, web, системы обмена сообщениями, распечатываемых или копируемых на различные устройства ввода-вывода
- Предотвращение утечки конфиденциальных данных путем блокирования процесса передачи в случае обнаружения нарушения политики безопасности
- Анализ и хранение данных для проведения расследований

Oracle IRM: преимущества

- Неавторизованные пользователи не могут получить доступ к информации
- Только авторизованные пользователи могут открывать или модифицировать документы в соответствии с их правами
- Вся работа с «запечатанной» информацией централизованно протоколируется
- Доступ к удалённо хранимой информации может быть централизованно отменён, например, если отношения с пользователем, работником по контракту, партнёром завершились (если он сделал эти копии, используя DVD, USB и др. средства)
- С помощью **Oracle IRM** возможно автоматически защитить любую информацию, отчуждаемую в виде отчетов из бизнес-приложений, например, ERP, CRM-систем
- **Oracle IRM** позволяет управлять информацией за межсетевыми экранами, даже когда информация хранится в сети других организаций или дома
- Удобство для конечного пользователя: не требуется ни переносить конфиденциальные документы в специальные хранилища или изменять процесс работы с документами

InfoWatch Traffic Monitor: преимущества

- Точная идентификация конфиденциальных данных благодаря совместному использованию различных технологий контентного анализа
- Надежная защита периметра корпоративной сети благодаря контролю над различными каналами утечки данных
- Поддержка различных типов и форматов файлов
- Предустановленные правила обработки и база контентной фильтрации, чтобы позволить компаниям немедленно воспользоваться всеми преимуществами решения по защите информации от внутренних угроз
- Централизованный архив для мониторинга текущей активности сотрудников, составления аналитических отчетов и проведения расследований
- Гибкая схема интеграции в IT-инфраструктуру компании

Функциональные возможности совместного решения

Совместное решение Oracle и InfoWatch позволяет:

- Выявлять конфиденциальную информацию, отправляемую за периметр сети предприятия в «незапечатанном» виде (т.е. не защищенную средствами Oracle IRM) при помощи комплексного анализа текста с использованием нескольких технологий:
 - Поиска текстов, похожих на известные конфиденциальные документы, при помощи цифровых отпечатков, снятых с текста документов, защищенных Oracle IRM.
 - Проактивного поиска конфиденциальной информации по категориям (финансы, персональные данные и резюме, информация о контрагентах и контрактах, отраслевые технологические документы и т.п.) на основе уникального лингвистического анализа. Это обеспечивает защиту конфиденциальной информации, которая еще не попала под защиту Oracle IRM.
 - Поиска алфавитно-цифровых объектов по преднастроенным шаблонам (номера паспортов, кредитных карт, номеров пенсионного страхования в РФ и др.).
 - Выделения текста из изображений для последующего анализа при помощи распознавания символов OCR – Optical Character Recognition. Это необходимо для анализа операций PrintScreen и пересылаемых рисунков/фотографий разных форматов.
- Контролировать различные каналы утечки данных: Интернет (форумы, блоги), web-mail, e-mail, ICQ и операции записи информации на отделяемые носители (флэшки, диски, смартфоны и т.п.).
- *Опционально:* при выявлении конфиденциальной информации, покидающей сеть предприятия в незащищенном средствами Oracle IRM виде, принудительно ее «запечатывать» или блокировать передачу в соответствии с политиками безопасности.
- *Опционально:* при обнаружении заданного количества инцидентов по одному пользователю за определенный промежуток времени – блокировать права пользователя на доступ к «запечатанным» документам до разбирательства.

Поддерживаемые форматы

Oracle IRM поддерживает:

- Microsoft Office 2000-2007 (Word, Excel and PowerPoint)
- Adobe Acrobat or Reader 6.0+
- Email: Microsoft Outlook 2000-2007, Lotus Notes 6.5-7.0 and Novell GroupWise 6.5-7.0
- Email: BlackBerry for Exchange and Domino, BES 4.1.4
- HTML and XML (Internet Explorer 6.0+)
- TXT and .RTF documents
- GIF, JPEG and PNG images

Открытые интерфейсы Oracle IRM позволяют защитить документы любого типа с помощью вызова стандартных Web-сервисов системы.

InfoWatch Traffic Monitor поддерживает:

- MS Office 97-2007 (DOC, DOCX, XLS, XLSX, PPT, PPTX)
- TIFF, JPEG, GIF, PNG
- EMF, WMF
- TXT, RTF
- PDF
- MDB
- HTML
- XML
- TNEF
- GZIP, BZIP2, TAR, ARJ, ZIP, SFX, RAR, LHA
- EXE
- MP3, WAV
- AVI, WMV

Преимущества совместного решения

- Поддержка всех основных версий Windows и MS Office, что существенно снижает издержки на внедрение решения.
- Поддержка как аутентификации с помощью MS Active Directory, так и внутренней аутентификации, что облегчает использование решения для внешних пользователей.
- Управление доступом на уровне ролей и шаблонов (контекстов безопасности), а не на уровне отдельных файлов и пользователей. Это повышает управляемость и масштабируемость (имеются внедрения IRM и DLP на более 60 тыс. пользователей).
- Возможность защиты большинства форматов документов (не только документов MS Office).
- Возможность контроля попытки хищения конфиденциальной информации с помощью перехвата копии экрана (например, Ctrl /PrintScreen).
- Изменение прав пользователей на документы без перекодирования файлов. Возможность отозвать права пользователей после того, как документы уже получены конечным пользователем.
- Клиентская часть **Oracle IRM** состоит из одного модуля, который может быть установлен централизованно.
- Поддержка поиска по защищенным документам.
- Предотвращение утечки конфиденциальных данных как похожих на защищенные документы, так и новых документов/текстов/ e-mail, еще не защищенных средствами **Oracle IRM**.
- Сертификация **Oracle IRM** и **InfoWatch Traffic Monitor** по требованиям безопасности информации в соответствии с руководящими документами РФ, в том числе для защиты персональных данных.

Контакты: