INFOWATCH TRAFFIC MONITOR

INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

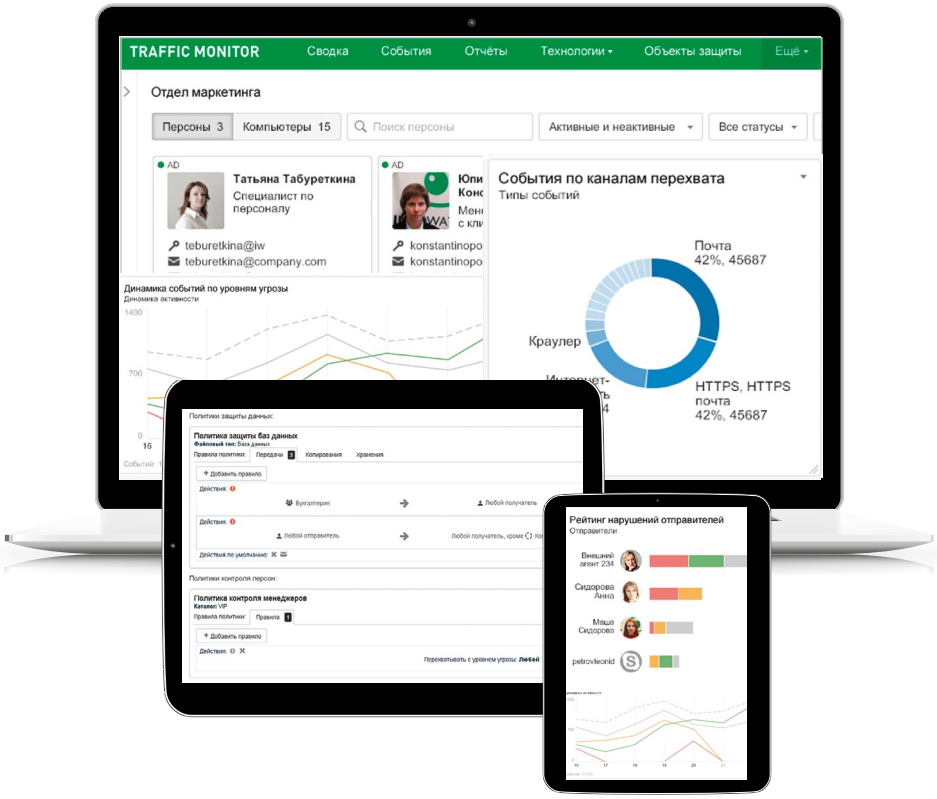
Защита предприятия от утечек информации и внутренних угроз

На сегодняшний день в компаниях различных сфер бизнеса количество внутренних атак превышает количество внешних. Собственные сотрудники оказываются серьезной угрозой и способны нанести огромный ущерб вследствие кражи корпоративной информации или ее утечки по неосторожности, а также коррупции, мошенничества, сговоров, воровства и саботажа.

Защитить компанию от утечек информации и внутренних угроз поможет InfoWatch Traffic Monitor – автоматизированная система контроля информационных потоков организации.

InfoWatch Traffic Monitor — единственное средство информационной безопасности, которое решает бизнес-задачи:

- помогает бизнесу получить уверенность в безопасности ценных и конфиденциальных данных
- дает понимание всех внутренних потоков информации в организации
- позволяет выявить сговоры, злоумышленников, лиц, занимающихся промышленным шпионажем, а также круг причастных лиц
- помогает осуществлять бизнес-разведку с целью контроля деятельности персонала и определения степени его лояльности к компании
- формирует доказательную базу по инцидентам для дальнейшего юридического расследования нарушений



Главной особенностью решения InfoWatch является вовлечение бизнес-подразделений в управление безопасностью — HR-служба, владельцы информации, топ-менеджеры. Это позволяет свести к минимуму угрозы со стороны собственного персонала, минимизировать риски.

InfoWatch Traffic Monitor — комплексное решение, которое охватывает организационные, технические и юридические вопросы обеспечения внутренней безопасности компании:

ОРГАНИЗАЦИОННЫЕ АСПЕКТЫ: Pre-DLP

- аудит состояния информационной безопасности в компании
- категоризация информационных ресурсов
- разработка регламентирующей документации
- внесение изменений в режим коммерческой тайны

ТЕХНИЧЕСКИЕ АСПЕКТЫ: DLP

- внедрение технических средств DLP
- настройка технических средств в соответствии с разработанными регламентами и отраслевой спецификой
- техническое сопровождение DLP-системы

ЮРИДИЧЕСКИЕ АСПЕКТЫ: Post-DLP

- юридически значимая база инцидентов
- получение криминалистически правильных цифровых доказательств правонарушения
- юридически грамотное сопровождение внутренних расследований

INFOWATCH TRAFFIC MONITOR

INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Предотвращение утечек конфиденциальной информации

Мониторинг, перехват и анализ всех информационных потоков осуществляется по наиболее распространенным каналам передачи данных и с ипользованием уникальных запатентованных технологий анализа.

КОНТРОЛИРУЕМЫЕ КАНАЛЫ ПЕРЕДАЧИ ДАННЫХ:

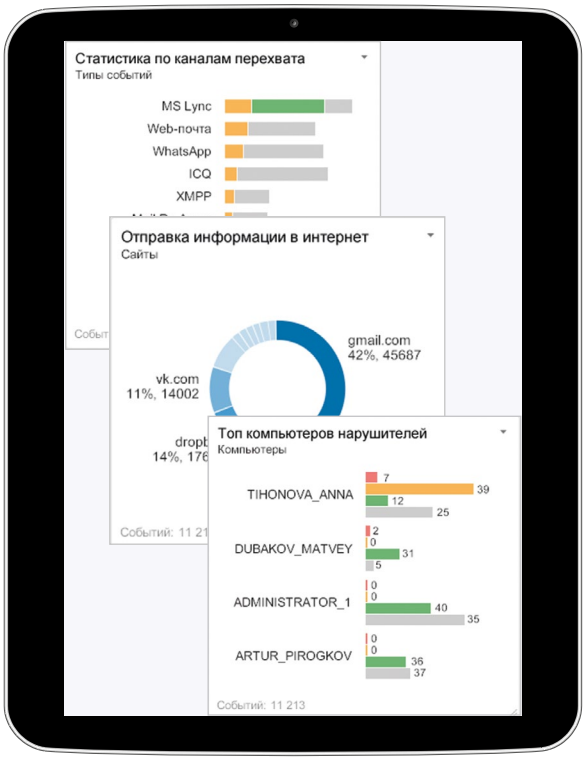
- корпоративные почтовые серверы (SMTP, POP3, IMAP, Lotus Domino), веб-почта
- интернет-ресурсы (HTTP, HTTPS, FTP)
- системы обмена сообщениями (ICQ, Skype, IM Yahoo, Mail.ru Агент и другие), а также корпоративная система обмена сообщениями Microsoft Lync
- голосовой трафик
- внешние устройства и порты на рабочих станциях
- мобильные устройства (Android, iOS, YotaPhone) - SMS, мессенджеры, почтовый и интернет-трафик

android iOS YOTAPHONE

- сетевые соединения на рабочих станциях
- облачные сервисы (Dropbox, Яндекс.Диск и др.)
- терминальные подключения Microsoft RDP, Citrix

CITRIX®

- локальные и сетевые принтеры



ТЕХНОЛОГИИ АНАЛИЗА ДАННЫХ

Лингвистический анализ
Метод, позволяющий точно детектировать коммерческие секреты в любых типах документов, используя обширный список технологий и базы контентной фильтрации (БКФ)

Базы Контентной Фильтрации (БКФ)
База данных, представляющая собой иерархически организованный список слов и выражений, наличие которых в документе позволяет определить тематику и степень конфиденциальности информации

Цифровые отпечатки
Технология, предназначенная для защиты больших по объему документов, содержание которых не изменяется или меняется незначительно

Анализатор шаблонов
Технология позволяет детектировать алфавитно-цифровые объекты по шаблону данных и эффективно выявляет факты пересылки персональных данных или финансовой информации

Детектор графических объектов
Технология позволяет определить наличие страниц паспорта гражданина РФ и кредитных карт в потоке перехваченных файлов

Детектор выгрузок из баз данных
Технология предотвращает утечки любой информации, хранящейся в базах данных (например, база клиентов).
Скорость анализа - 54 млн. знаков в секунду

Детектор заполненных анкет
Технология позволяет отслеживать передачу по сетевым каналам анкет (в том числе, отсканированных и заполненных от руки), содержащих персональные данные

Детектор печатей
Технология, предназначенная для отслеживания движения и передачи отсканированных документов, содержащих изображения эталонных печатей

Optical Character Recognition (OCR)
Технология распознавания изображений, с целью извлечения из них текстовой информации для дальнейшего анализа

Комбинированные объекты защиты
InfoWatch Traffic Monitor выносит вердикт о конфиденциальности перехваченной информации, используя результаты анализа не одной, а сразу нескольких технологий. Данный метод позволяет применять комбинацию различных техник защиты для сложных типов данных, значительно снижая число ложноположительных срабатываний

INFOWATCH TRAFFIC MONITOR

INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Защита от внутренних угроз

InfoWatch Traffic Monitor позволяет организовать мониторинг и перехват всех электронных коммуникаций на рабочих станциях, ноутбуках и мобильных устройствах сотрудников. Интеллектуальная платформа системы выявляет подозрительную активность сотрудников компании, устанавливая факты воровства, мошенничества, коррупции, сговоров и саботажа, позволяет идентифицировать злоумышленников и всех причастных лиц, участвующих в незаконной деятельности. Вся перехваченная информация хранится в единой базе инцидентов для дальнейшего расследования.

В результате запуска в эксплуатацию системы InfoWatch ОАО «Газпром автоматизация» удалось решить все поставленные задачи по защите информации нашей организации от утечек.

Мятлев В.А., И.О. заместителя генерального директора по корпоративной защите и кадрам

Продукт InfoWatch Traffic Monitor был выбран благодаря уникальным технологиям анализа, которые не смогла предложить никакая другая DLP-система.

Карицкий А.А., директор дирекции информационных технологий ОАО «НМТП»

Мониторинг сотрудников в «группе риска»

Благодаря встроенным инструментам взаимодействия с HR-службой, InfoWatch Traffic Monitor учитывает больше данных для формирования картины угроз, чем традиционные DLP-системы. Продукт позволяет настраивать и применять особые целевые политики контроля персонала, входящего в так называемую «группу риска» с созданием специальных отчетов по активности подобных сотрудников.

К примеру, HR-специалист компании может включить в «группу риска» сотрудников, находящихся на испытательном сроке или планирующих уволиться, и к ним автоматически будет применяться более строгая политика безопасности.

Нарушители – «как на ладони»

InfoWatch Traffic Monitor идентифицирует нарушителей и круг причастных лиц, ведет статистику нарушений, что позволяет предупредить наиболее опасные угрозы, включая комбинированные (внутренние и внешние нарушители, действующие в сговоре). Вся информация хранится в единой базе для дальнейшего расследования инцидентов, построения отчетов и оперативного реагирования на инцидент.

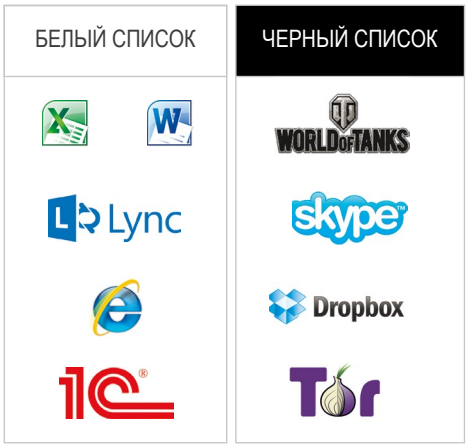
Продукт представляет информацию о нарушениях в разрезе:

- выбранного периода времени
- уровня нарушения: низкий, средний, высокий
- типов нарушенных правил: передачи, хранения и копирования

Борьба с бездельниками

InfoWatch Traffic Monitor контролирует приложения, запускаемые сотрудниками. Настраивая «черные» и «белые» списки, офицер информационной безопасности может разрешать или запрещать использование тех или иных программ. Пользователи больше не будут часами переписываться в мессенджерах или играть в компьютерные игры, а злоумышленники не смогут запустить вредоносное программное обеспечение на рабочей станции.

- Запрет запуска приложений из списков («черный» список)
- Запрет запуска приложений, не входящих в списки («белые» списки)
- Правила по контролю приложений могут применяться как на рабочую станцию, так и на сотрудника (группы сотрудников)
- Автоматическое формирование списков приложений



Система защиты от внутренних угроз, установленная в банке, должна контролировать все ключевые каналы передачи информации, обладать высокой производительностью, а также передовыми технологиями анализа. Поэтому в 2007 году в «Нордеа Банке» было внедрено решение InfoWatch Traffic Monitor.

Михаил Генис, заместитель председателя правления «Нордеа Банка»

Компоненты программного комплекса InfoWatch Traffic Monitor были установлены на серверах и рабочих станциях Банка Москвы, и с этого момента в банке осуществляется мониторинг исходящего почтового и web-трафика, контроль копирования информации на внешние устройства, а также архивирование содержимого корпоративной электронной почты.

Окулесский В.А., начальник ОЗИ СБ

INFOWATCH TRAFFIC MONITOR

INFOWATCH®
МЫ РАБОТАЕМ, ЧТОБЫ ЗАЩИЩАТЬ

Контроль мобильных сотрудников

InfoWatch Traffic Monitor осуществляет:

- контроль рабочей активности сотрудников через мобильные устройства под управлением iOS, Android и т. д.
- мониторинг информации на ноутбуках в периметре и за пределами компании: агентская часть продукта продолжает работать, даже когда рабочие ноутбуки вынесены за пределы компании, и передает полученную информацию в подсистему анализа при их возвращении в корпоративную сеть
- благодаря технологии контроля сетевых соединений, ноутбуки, находящиеся за периметром компании, могут выходить в Интернет только через шлюз корпоративной сети, что гарантирует контроль всего сетевого трафика

Решение дает возможность полноценно пользоваться смартфонами и планшетами, не ограничивая продуктивность сотрудников, при этом снижает риск утечки конфиденциальных данных через мобильный канал.

«Сфотографировал экран» больше не работает

На протяжении долгого времени «фотографирование экрана» оставалось любимым способом обхода средств защиты информации. Защитив корпоративные смартфоны с помощью InfoWatch Traffic Monitor все фотографии, сделанные на смартфон сотрудника, будут подвергаться анализу на предмет содержания конфиденциальной информации и сохраняться в архив на сервере InfoWatch Traffic Monitor.

Повышайте продуктивность

На мобильное устройство устанавливается программа-агент, которая перехватывает веб-трафик, сообщения, фотографии и отправляет в модуль InfoWatch Device Monitor всю информацию для дальнейшего анализа, архивации и принятия решения по инциденту.

Исходящие сообщения электронной почты и интернет-публикации анализируются с применением полного спектра технологий InfoWatch Traffic Monitor для выявления нарушений политик информационной безопасности организации.

Помимо этого, можно управлять списком приложений, разрешенных к использованию на смартфонах и планшетах вашей организации, запрещая установку игр и потенциально опасных приложений.

МОБИЛЬНАЯ БЕЗОПАСНОСТЬ

	Поддерживаемые устройства	
Функциональные возможности	***Android***	***iOS***
Контроль камеры Перехват и теневое копирование снятых фотографий	+	+
Контроль сообщений Перехват и теневое копирование входящих и исходящих сообщений	+	+
Контроль iMessage	не применимо	+
Анализ и архивирование переписки в WhatsApp Messenger	+	+
Контроль запуска приложений • «Белые» списки приложений, разрешенных для использования сотрудниками на мобильных устройствах • Запрет использования игр, развлекательных приложений и прочих «пожирателей рабочего времени» с помощью «черного» списка приложений	+	+
Контроль электронной почты Перехват и теневое копирование почтового трафика • Контроль сообщений и вложенных файлов, отправленных через почтовые клиенты по протоколу SMTP, POP3, IMAP	+	отсутствует
Контроль веб-трафика • Перехват и теневое копирование HTTP/S трафика • Контроль сообщений и вложений, отправленных через сервисы веб-почты (Mail.ru, Gmail, Яндекс.Почта и т.п.) • Контроль публикации сообщений и загрузки файлов через веб-ресурсы,социальный сети, облачные хранилища (Facebook, Вконтакте, Яндекс.Диск, Dropbox и т.п.)	+	отсутствует

INFOWATCH TRAFFIC MONITOR

INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

Архитектура

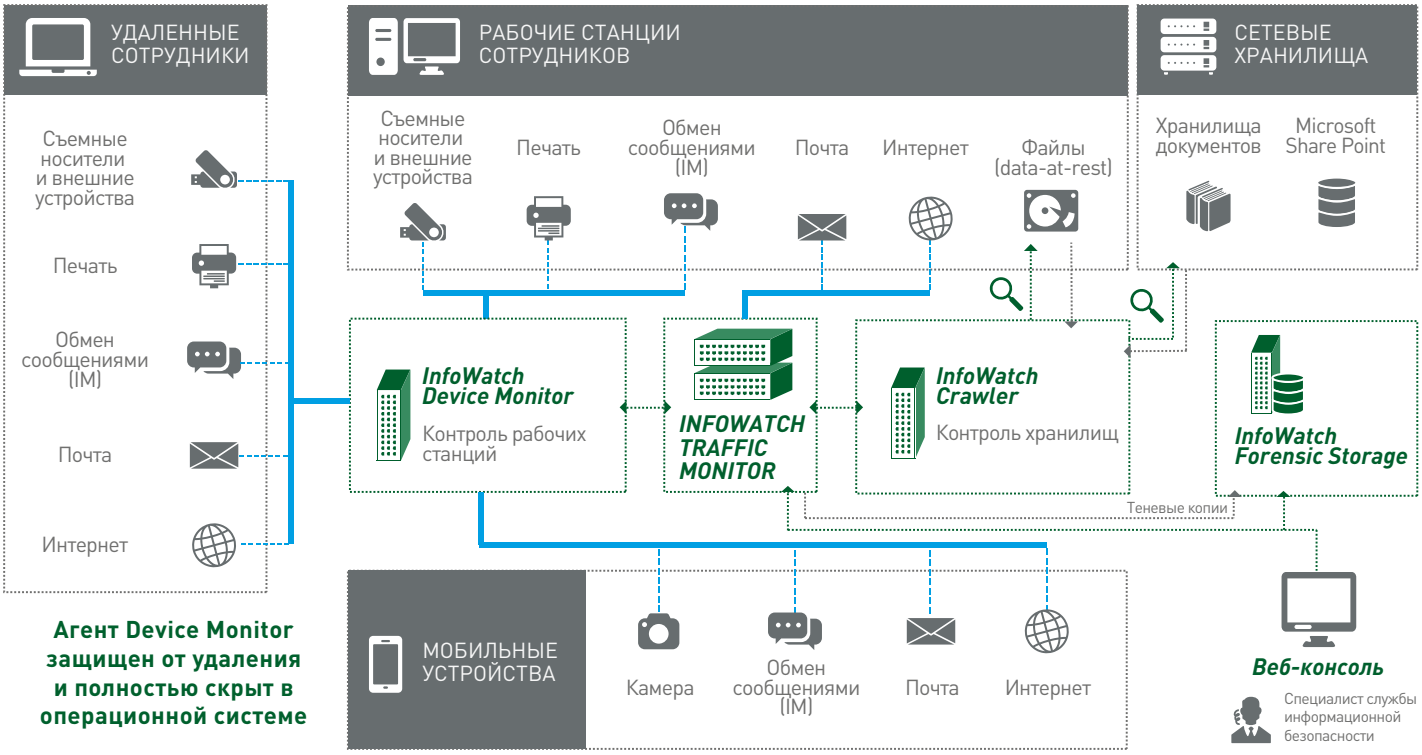
InfoWatch Traffic Monitor состоит из нескольких модулей:

1. **InfoWatch Traffic Monitor**- модуль для контроля сетевых каналов передачи данных

2. **InfoWatch Device Monitor** - модуль для защиты рабочих станций, осуществляющий контроль печати, копирования документов на съемные носители, а также контроль портов и съемных устройств. Программные агенты Device Monitor создают теневые копии документов и передают их на сервер Traffic Monitor для дальнейшего анализа.

3. **InfoWatch Crawler** - модуль для контроля информации в общедоступных сетевых хранилищах и системах документооборота, осуществляет сканирование и применение политик к информации, хранящейся «в покое», а также поддерживает в актуальном состоянии эталонные документы и выгрузки. InfoWatch Crawler создает теневые копии найденных документов и передает их на сервер Traffic Monitor для дальнейшего анализа и применения политик

4. **InfoWatch Forensic Storage** - специализированное хранилище, содержащее архив всех информационных потоков организации, в том числе нарушения политик безопасности и факты утечек конфиденциальной информации; является юридически значимой доказательной базой при проведении внутрикорпоративного расследования инцидентов и в ходе судебных разбирательств.



Расследование инцидентов и отчетность

Централизованный архив, содержащий все перехваченные данные, представляет собой надежную доказательную базу для глубокого анализа и расследования инцидентов.

Преимущества

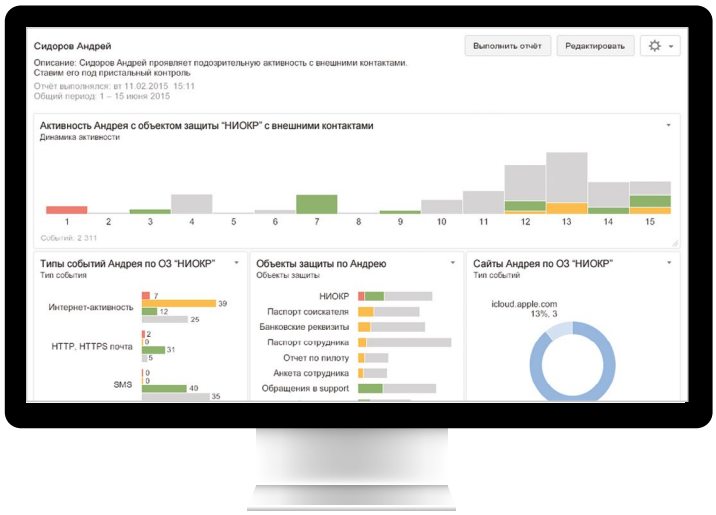
- Неограниченный объем хранимой информации: ограничивается лишь возможностями СУБД и аппаратной платформы
- Поддержка нескольких СУБД - Oracle, PostgreSQL
- Полнотекстовый поиск на базе поисковой машины Sphinx: по содержимому перехваченных сообщений и вложений
- Масштабируемость: может использоваться в организациях со сложной филиальной структурой
- Создание зон ответственности: позволяет разграничить доступ сотрудников к хранимой информации
- Ограничение просмотра содержимого: позволяет соблюдать право на тайну переписки
- Предварительный анализ выгружаемых данных: выгрузка хранимой информации возможна как в исходном виде, так и с результатами анализа
- Мониторинг активности сотрудников в режиме «реального времени»

INFOWATCH TRAFFIC MONITOR

INFOWATCH®
МЫ РАБОТАЕМ,
ЧТОБЫ ЗАЩИЩАТЬ

ОТЧЕТНОСТЬ

InfoWatch Traffic Monitor обладает уникальной системой отчетности, позволяющей офицеру безопасности и другим заинтересованным лицам получать наглядную оперативную сводку по выявленным угрозам, нарушителям и связям между ними, каналам передачи информации, объектам защиты и многим другим параметрам. С помощью графического конструктора и системы виджетов можно создать любое удобное представление данных и включить в отчет именно ту информацию, которая требуется в данный момент.



Преимущества InfoWatch Traffic Monitor

- Высокая скорость анализа данных
- Точность детектирования конфиденциальных данных
- Минимальное количество ложных срабатываний
- Кастомизация под специфику бизнеса (отраслевые решения)
- Обеспечивает соответствие ряду требований регуляторов (№152-ФЗ «О персональных данных», № 273-ФЗ «О противодействии коррупции», Постановления Правительства РФ №1119 «Об утверждении требований к защите ПДн при их обработке в информационных системах ПДн», Приказа №21, требованиям Межгосударственного стандарта «Средства Вычислительной Техники» по 5 классу защищённости)
- Российская разработка, обладающая всеми необходимыми лицензиями и сертификатами: ФСТЭК, ФСБ России, Газпромсерт, аккредитация ЦБ РФ и др.

Для крупного бизнеса

ВЕРСИЯ ENTERPRISE

- Для крупных компаний и компаний с географически-распределенной филиальной структурой
- Мощное решение с высокой производительностью и отказоустойчивостью
- Неограниченный срок хранения данных в архиве
- Модульная структура: комплектация и состав продукта определяется клиентом

Для среднего бизнеса

ВЕРСИЯ STANDARD SOLUTION

- Для небольших компаний и организаций среднего размера (до 500 ПК)
- Оптимизирована для работы в небольших организациях: требует минимальных настроек
- Ограниченный срок хранения данных в архиве
- Полностью готовое к установке и внедрению решение