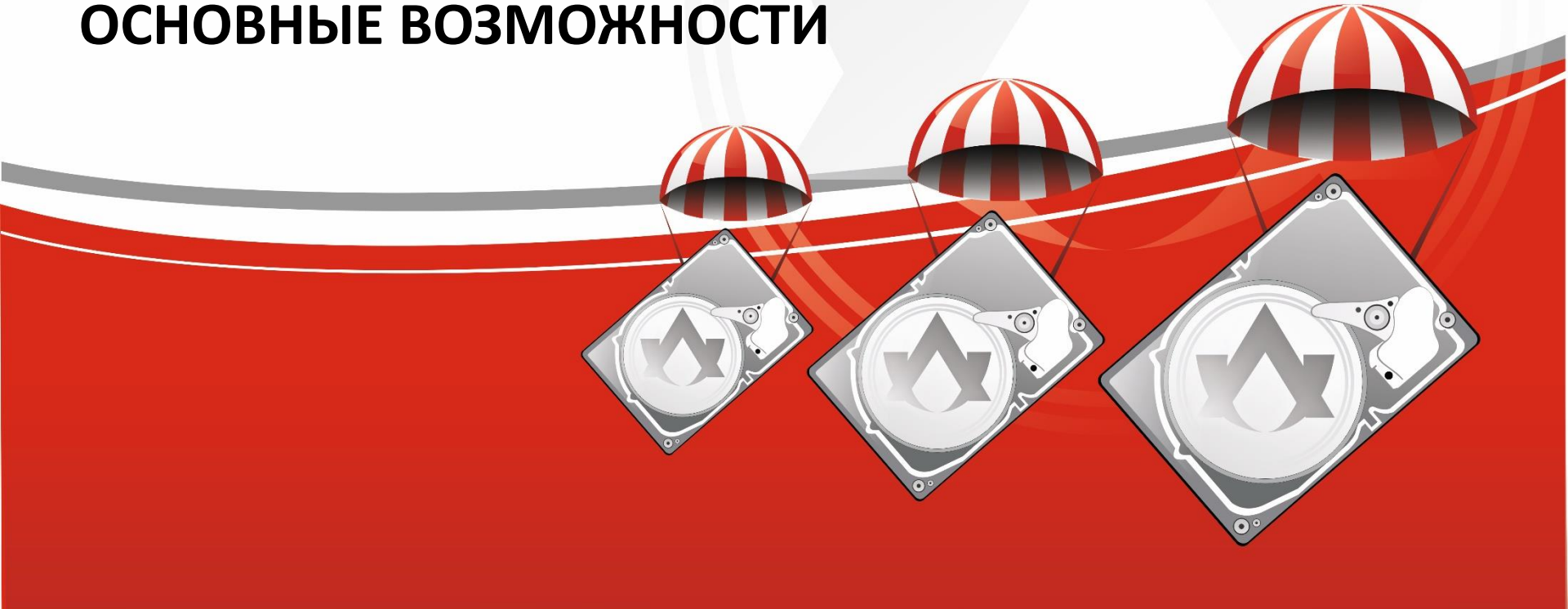
Atlansys Software

Atlansys WHITECLOUD

ОСНОВНЫЕ ВОЗМОЖНОСТИ

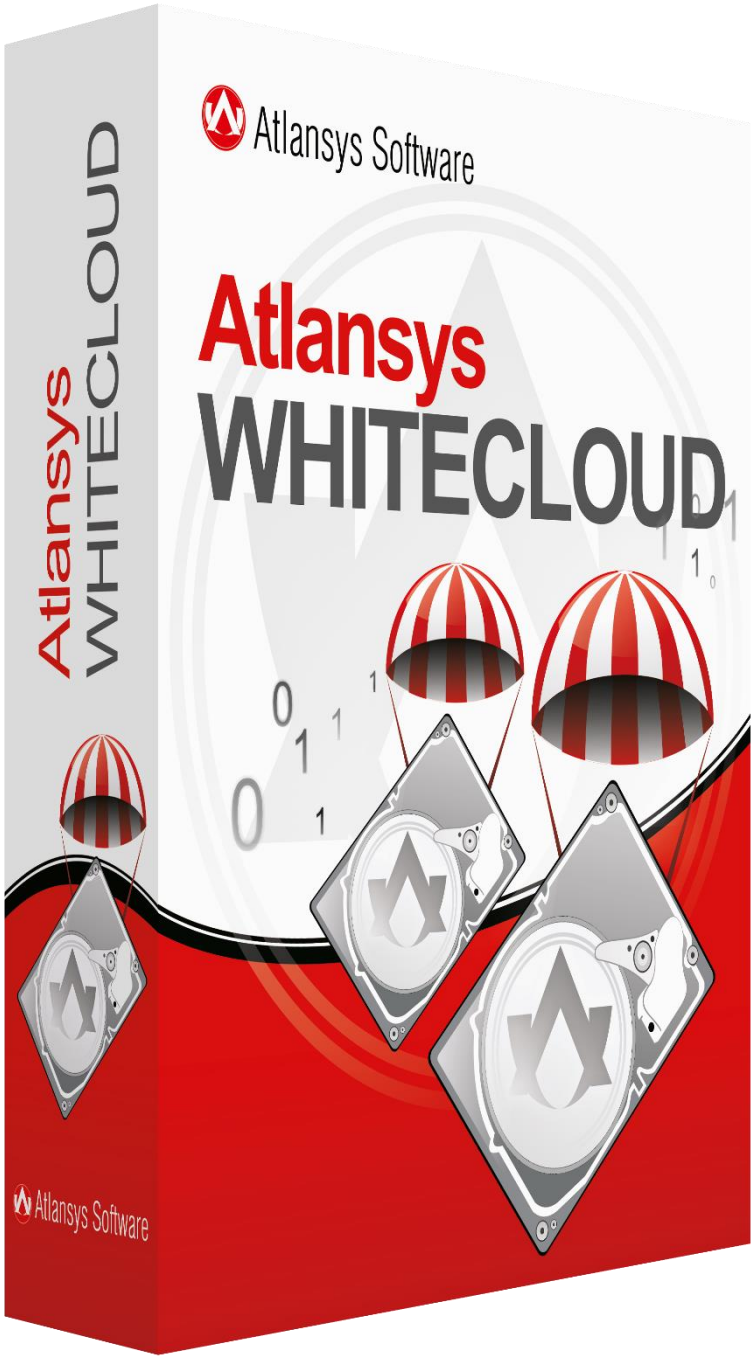


ATLANSYS WHITECLOUD

- ***Atlansys WhiteCloud – отечественное решение*** *шифрования и хранения КОРПОРАТИВНОГО КОНТЕНТА (в том числе электронных версий документов) с использованием собственного защищенного облачного хранилища, размещаемого на собственных серверах или серверах удаленного ЦОД.*

- ***Заказчик является 100% владельцем своих данных*** *и имеет полный контроль над ними без возможности доступа третьих лиц, включая администратора сервисов Atlansys WhiteCloud.*

- ***Atlansys WhiteCloud*** *- это инвестиции. На базе Atlansys WhiteCloud можно решать не только внутрикорпоративные задачи по информационной безопасности в рамках интеграции в СУИБ, но и создавать коммерческие сервисы для партнеров и контрагентов.*

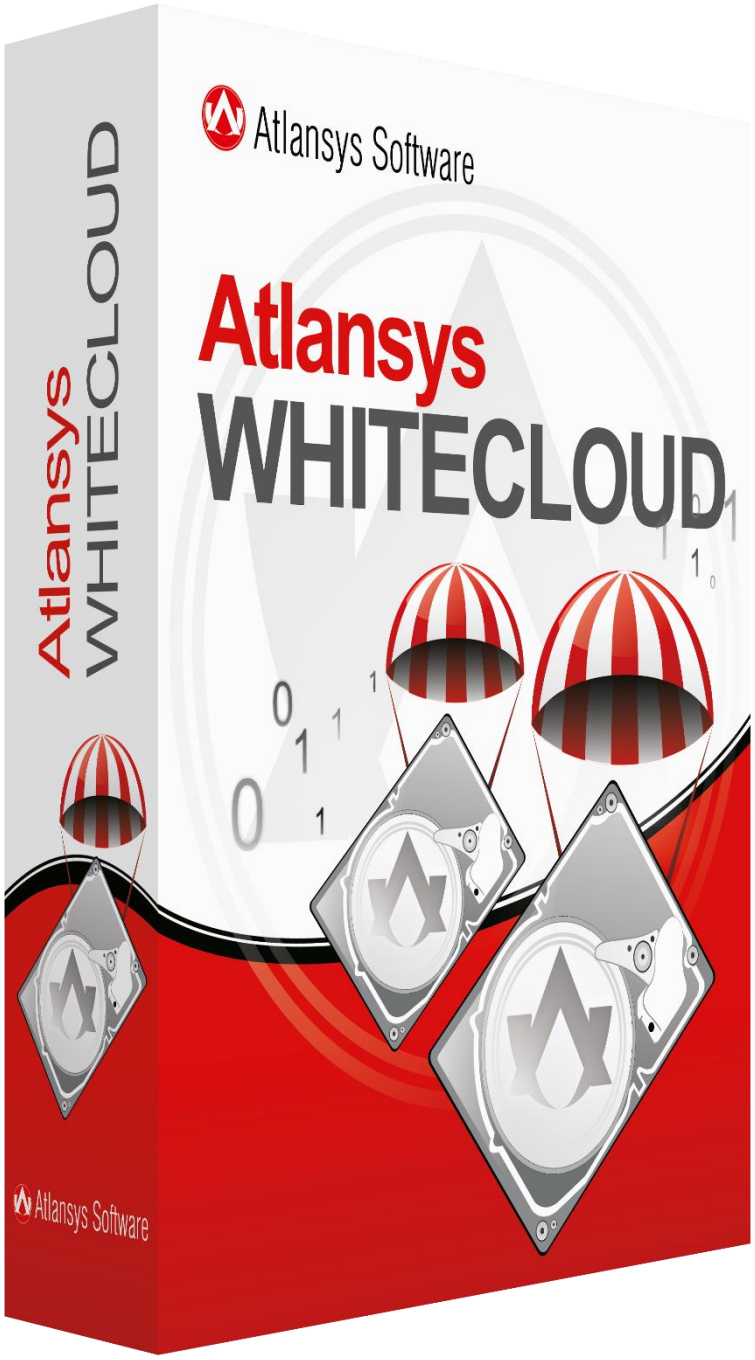


ATLANSYS WHITECLOUD ПРЕИМУЩЕСТВА

- ***Средство защиты информации Atlansys WhiteCloud имеет сертификат соответствия ФСТЭК России №2987*** *по 4 уровню контроля недекларированных возможностей (НДВ) и технических условий (ТУ), что позволяет использовать данное решение для построения автоматизированных систем до класса 1Г включительно.*

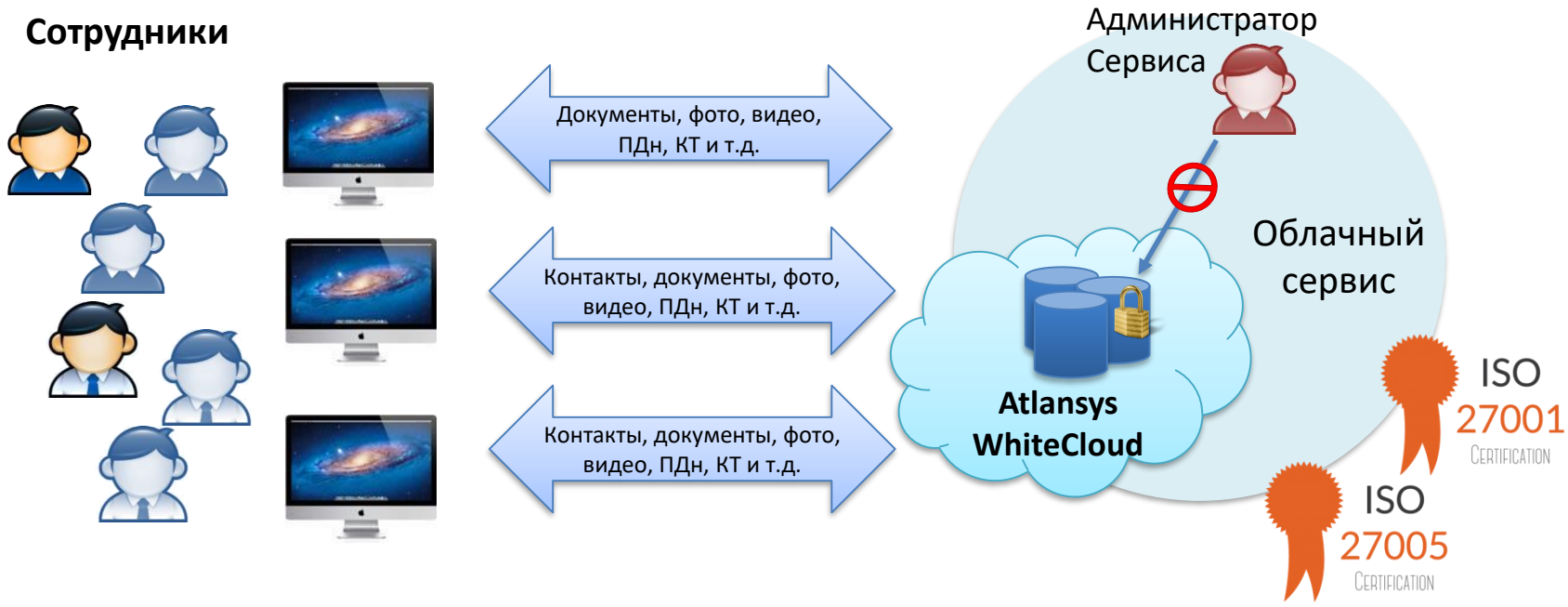
- ***Решение Atlansys WhiteCloud зарегистрировано в едином реестре Минкомсвязи России*** *российских программ для ЭВМ и баз данных №2020 от 08 октября 2016 года.*

- ***Atlansys WhiteCloud – лучшее решение*** *по версии журнала PC MAGAZINE RE 2012 и «Продукт года» по версии Softool 2016.*



ATLANSYS WHITECLOUD
РЕШЕНИЕ ДЛЯ КОРПОРАТИВНОГО ЗАКАЗЧИКА

Все сотрудники имеют защищенные рабочие места с возможностью безопасной удаленной работы со своими документами



Atlansys WhiteCloud *- внутрикорпоративное защищенное хранилище для безопасного хранения и обмена любой информации между сотрудниками, в том числе информации ограниченного доступа*

ATLANSYS WHITECLOUD
РЕШЕНИЕ ДЛЯ КОРПОРАТИВНОГО ЗАКАЗЧИКА

Все данные сотрудников Заказчика хранятся в «облаке». ЗАЩИЩЕННО!

Преимущества

- ✓ *Интеграция в корпоративную СУИБ.*
- ✓ *Защита ПДн и коммерческой тайны от внешних и внутренних нарушителей.*
- ✓ *Снижение стоимости владения системой и затрат на ее эксплуатацию.*
- ✓ *Повышение уровня управляемости защищаемой информации.*
- ✓ *Выполнение требований ФЗ и регуляторов.*

Сервисы

- ✓ *Создание единого распределённого защищенного хранилища для любого контента и пользовательских данных сотрудников.*
- ✓ *Организация безопасного обмена документами между сотрудниками на корпоративном портале в «облаке».*
- ✓ *Защита отчетов и протоколов событий с различных систем мониторинга в «облаке» для организации безопасного доступа к ним должностных лиц из любой точки мира.*
- ✓ *Хранение истории документов, работа с документами в off-line режиме.*

Управление и Интеграция

- ✓ *Интеграция с MS ActiveDirectory и поддержка инфраструктуры открытых ключей PKI*
- ✓ *Централизованное управление профилями и квотами пользователей.*
- ✓ *Удаленная работа с данными с возможностью безопасного совместного доступа.*
- ✓ *Процедуры управления и восстановления ключей.*
- ✓ *Протоколирование и экспорт событий.*

ATLANSYS WHITECLOUD
РЕШЕНИЕ ДЛЯ КОНТРАГЕНТОВ / АБОНЕНТОВ

Новый сервис по безопасному хранению и обмену информации между контрагентами/абонентами и Заказчиком / Оператором

Atlansys WhiteCloud *– «облачный»/платный сервис по безопасному хранению и совместному доступу к любому контенту для контрагентов/абонентов и сотрудников Заказчика/Оператора из любой точки мира.*

При этом Заказчик/Оператор является собственником хранилища данных, в отличии, например, от того же Яндекс диска или Dropbox, т.е. данные клиентов недоступны третьим лицам.

ATLANSYS WHITECLOUD
РЕШЕНИЕ ДЛЯ КОНТРАГЕНТОВ / АБОНЕНТОВ

Преимущества

- ✓ *Создать платный «облачный» сервис по безопасному хранению и совместному доступу к любому контенту для b2b/b2g клиентов Оператора из любой точки мира.*
- ✓ *WhiteCloud предоставляет пользователям личные защищенные хранилища данных, доступ к информации в которых отсутствует даже у администраторов сервиса.*
- ✓ *Удаленная работа с защищенными данными с возможностью безопасного совместного доступа из любой точки мира.*

Сервисы

- ✓ *Единая система защищенного файлового документооборота (документы, фото, видео, КТ, ПДн) для контрагентов/абонентов.*
- ✓ *Защита информационных систем (1С Бухгалтерия и др.) и бизнес-процессов контрагентов/абонентов.*
- ✓ *Подключение внешних ресурсов и облачных хранилищ на базе Яндекс к сервису WhiteCloud с шифрованием на стороне контрагентов/абонентов.*
- ✓ *Поддержка мобильных платформ (iOS, Android).*

Управление и интеграция

- ✓ *Централизованное управление профилями и квотами пользователей.*
- ✓ *Интеграция с различными информационными и биллинговыми системами.*
- ✓ *Процедуры управления и восстановления ключей.*
- ✓ *Мониторинг и протоколирование событий.*

ATLANSYS WHITECLOUD
СИСТЕМА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ISO 27001

Риски хранения данных в облачном хранилище	Примеры	Контрмеры, реализуемые с помощью Atlansys WhiteCloud
Конфиденциальность Один из важнейших аспектов рисков безопасности при хранении и пересылке данных в сети Интернет, то есть это гарантия того, что данные не стали доступными для посторонних лиц.	Злоумышленник, получивший несанкционированный доступ к хранилищу данных пользователя; Постороннее лицо, получившее доступ к компьютерному оборудованию пользователя; Сотрудник, не обладающий полномочиями для доступа к данной информации пользователя.	✓ Шифрование - защитный механизм, позволяющий шифровать данные пользователя на стороне клиента WhiteCloud, которые кэшируются, и синхронизируются с хранилищем, а затем в зашифрованном виде передаются по защищенному каналу на удаленный сервер WhiteCloud в ЦОД. Шифрование и синхронизация данных с удаленным сервером осуществляются для пользователя прозрачно. ✓ Аутентификация - только авторизованные пользователи имеют доступ к данным, которые хранятся в «облаке». Необходимо наличие сертификата с закрытым ключом авторизованного пользователя для доступа к клиенту WhiteCloud и данным внутри хранилища. ✓ Для совместного доступа к файлам - пользователь, пожелавший поделиться своими данными, получает открытый ключ другого пользователя из хранилища сертификатов, которым шифруется выбранный для общего доступа файл, и потом возвращает его на сервер, где он уже будет помещен в хранилище получателя файла. При этом пользователь может работать с защищенным хранилищем на рабочей станции, ноутбуке у себя в офисе или на мобильном устройстве в любой точке мира через вэб-клиент используя закрытый ключ в браузере в специальном java-апплете. ✓ Физическая безопасность - доступ к физической инфраструктуре, используемой для хранения, ограничен, она контролируется и закрыта для посторонних лиц. Контроль целостности программы и компонентов WhiteCloud.
Доступность Возможность за приемлемое время получить требуемую информационную услугу, то есть получить доступ к данным на облачных хранилищах в любое время без задержек с любого устройства.	Сотрудник отсутствующий на рабочем месте в связи с отпуском или командировкой, может предоставить удаленный доступ к необходимым документам другому авторизованному сотруднику; Сотрудник может предоставить свои файлы для общего доступа другим пользователям системы.	
Целостность гарантия того, что данные будут храниться правильно (актуальность и непротиворечивость информации).	Компьютерный вирус, вредоносное ПО, ошибки в коде или логике работы облачных хранилищ, ввод неверных или измененных данных злоумышленником	

ATLANSYS WHITECLOUD
УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ISO 27005

Источник	Пример воздействия угрозы	Контрмеры, реализуемые с помощью WhiteCloud
Разработчик ПО	Ошибки в коде или в логике работы облачного хранилища WhiteCloud, которые сложно идентифицировать и исправить обычным пользователям.	▪ В рамках сертификации был проведен контроль отсутствия недекларированных возможностей программного обеспечения, который предполагает глубокое исследование ПО и связан с анализом как исполняемого кода, так и исходных текстов программ. Наличие у компании разработчика лицензий ФСТЭК, ФСБ. ▪ Система самодиагностики для быстрого поиска ошибок и сбоев. ▪ Возможность автономной работы клиента WhiteCloud по средствам локального кэширования шифрованных данных на стороне клиента и их синхронизирования с хранилищем на сервере WhiteCloud в ЦОД позволяет при возобновлении работоспособности сервера хранилищ или канала связи передать измененные данные с клиента в шифрованном виде в хранилище на сервере. ▪ Шифрование данных пользователя происходит на стороне клиента WhiteCloud. Гарантией защищенности хранилища выступает шифрование хранимых файлов индивидуальным ключом для каждого пользователя. Только авторизованные пользователи имеют доступ к данным, которые хранятся в «облаке». Необходимо наличие сертификата с закрытым ключом авторизованного пользователя для доступа к клиенту WhiteCloud и данным внутри хранилища. Поддержка электронных ключей (JaCarta, eToken, ruToken и т.д.) ▪ Данная система допускает создание мастер-ключа, который позволит администратору безопасности системы при необходимости перешифровать файлы хранилища пользователя для другого закрытого ключа или пароля (т.е. восстанавливать доступ к данным в хранилище при потере сертификата или пароля пользователя). ▪ Использование усиленной защиты закрытого ключа на мобильном устройстве в виде пароля, а также пин-кода на аппаратном ключевом носителе (JaCarta, eToken, ruToken и т.д.), не дает возможности злоумышленнику получить доступ к данным в хранилище.
Аппаратно-программный сбой и конфликты с другим ПО	Отказ в обслуживании, некорректная работа (выход из строя сервера хранения данных, потеря канала связи)	
Администратор хранилищ	Несанкционированный доступ к хранилищу на сервере, содержащему конфиденциальные данные пользователя.	
Пользователь хранилищ	Несанкционированный доступ посторонних лиц к данным на стороне клиента; Потеря доступа к данным при утере пароля или сертификата,	
Злоумышленник	Потеря или кража мобильных устройств, eToken.	

ATLANSYS WHITECLOUD ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Шифрование данных

- *Данные шифруются на стороне клиента.*
- *Алгоритм шифрования ГОСТ (возможно применение зарубежных алгоритмов).*
- *Для шифрования используется пароль или сертификат (из реестра или из аппаратного ключа).*

Шифрование канала

- *Канал шифруется в момент установки соединения.*
- *Используется стандартная библиотека openssl.*

Аутентификация и авторизация

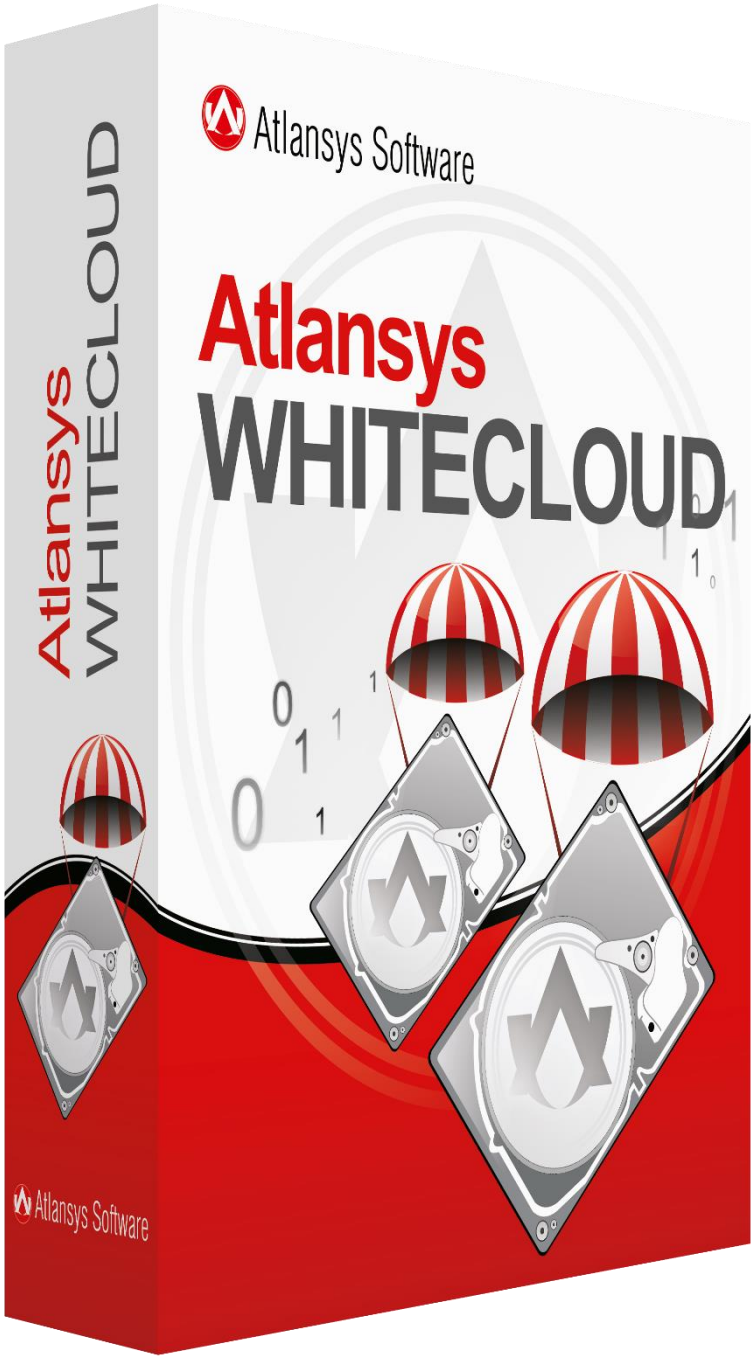
- *2 способа аутентификации: внутренняя БД пользователей и пользователи Active Directory. Для пользователей Active Directory есть возможность аутентификации с помощью пароля или с помощью сертификата на выбор.*

Протоколирование событий

- *На сервере в БД хранятся события от всех пользователей (вход/выход из системы, добавление/удаление/редактирование файла и т.д.). Администратор системы имеет возможность просмотра и анализа списка событий.*

Поддержка версий документов

- *Хранение предыдущих версий файла осуществляется на сервере. Пользователь может откатиться на любую предыдущую версию файла.*



ATLANSYS WHITECLOUD ФУНКЦИОНАЛЬНЫЕ ВОЗМОЖНОСТИ

Восстановление ключей

- *Восстановление утраченного пароля или сертификата осуществляется с помощью мастер-сертификата, который задается на этапе установки сервера. Назначение нового пароля или сертификата.*

Совместный доступ к файлам.

- *Пользователь может предоставить свои файлы для общего доступа другим пользователям системы. Другие пользователя увидят этот файл в своем хранилище и могут работать с ним так, как и со своими файлами.*

Совместный доступ к папкам. Общие папки

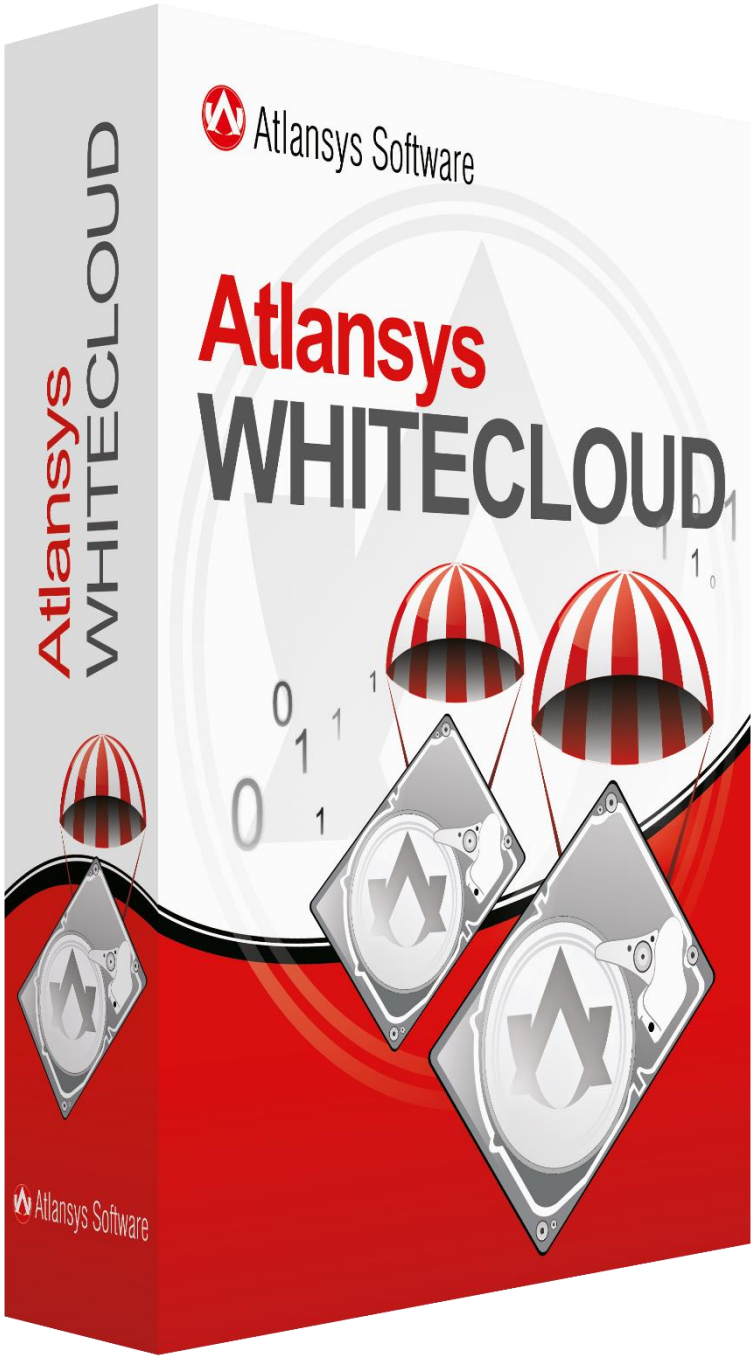
- *Хранение, обработка и обмен общими файлами и папками в защищенном режиме между автоматизированными пользователями с разграничением прав доступа.*

Работа в автономном режиме

- *При отсутствии связи с сервером пользователь может продолжать работу. При этом все модифицированные файлы сохраняются в локальном кэше. При появлении связи с сервером, происходит синхронизация.*

Управление пользователями, группами и их квотами

- *Администратор системы имеет возможность добавлять/удалять пользователей (при аутентификации через внутреннюю БД), добавлять/удалять группы пользователей. Квоты задаются при настройки групп, пользователей.*



ОСНОВНЫЕ ЗАКАЗЧИКИ ATLANSYS SOFTWARE

МТС

Защищено: 12 000 рабочих мест

МГТС

Защищено: 4 000 рабочих мест

COMSTAR

Защищено: 7 500 рабочих мест

БАШНЕФТЬ
АКЦИОНЕРНАЯ НЕФТЯНАЯ КОМПАНИЯ

Защищено: 2 000 рабочих мест

РОССЕТИ

МИНИСТЕРСТВО ЗДРАВООХРАНЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

МИНИСТЕРСТВО ФИНАНСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОЧТА РОССИИ

sochi.ru 2014

Олимпийский стадион «ФИШТ»

METRO

vancouver 2010

РТИ

НТВ плюс

MEDSI
сеть клиник

> 3000 КОМПАНИЙ ИСПОЛЬЗУЮТ РЕШЕНИЯ АТЛАНСИС

ОСНОВНЫЕ ЗАКАЗЧИКИ ATLANSYS SOFTWARE

МТС - Защищено 12 000 рабочих мест и более 30 серверов.

- ✓ *Защита от НСД при хранении коммерческой тайной на рабочих станциях, vip-ноутбуках – ФЗ №98 ст.10 п.2*
- ✓ *Безопасный обмен коммерческой тайной с партнерами в рамках NDA-соглашения - ФЗ №98 ст.10 п.2*
- ✓ *Централизованное управление и хранение ключей пользователей – ISO27001: A12.3.2*
- ✓ *Централизованное управление действиями пользователей при работе с криптографическими операциями – ISO27001: A12.3.1*
- ✓ *Гарантированное уничтожение конфиденциальной информации – ФЗ №98 ст.10 п.2*

Завод имени Дегтярева - Защищено 4 000 рабочих мест.

- ✓ *Создание единого защищенного хранилища с подключением внешних файловых ресурсов для разграничения прав доступа к корпоративным ресурсам Завода и защищенным доступом к ним со стороны подрядчиков.*

Министерство Здравоохранения РСО-Алания - Защищено 100 серверов.

- ✓ *Защита файловых серверов и серверов баз данных от внешних и внутренних нарушителей.*
- ✓ *Выполнение требований регуляторов при обработке ПДн в ИСПДн.*
- ✓ *Централизованное управление процедурами шифрования – ISO27001: A12.3.1*
- ✓ *Защита ключей шифрования от потери и кражи – ISO27001: A12.3.2*

ОСНОВНЫЕ ЗАКАЗЧИКИ ATLANSYS SOFTWARE

РТИ Системы - Защищено 1000 рабочих мест.

- ✓ *Шифрование системного раздела на ноутбуках и рабочих станциях сотрудников.*
- ✓ *Контроль и защита внешних носителей в компании.*
- ✓ *Централизованное управление процедурами шифрования и восстановление доступа.*

Metro Cash and Carry - Защищено 1 000 рабочих мест.

- ✓ *Защита системного раздела и базы данных ИСПДн на кассах под Windows Embedded в соответствии с законодательством РФ для прохождения проверки регулирующими органами при обработке ПДн с уровнем защищенности 4УЗ, 3УЗ, 2УЗ.*

Российские сети - Защищено 1000 рабочих мест.

- ✓ *ГОСТ Шифрование почтовых хранилищ MS Exchange 2013. Защита от НСД третьих лиц, включая администратора сервера.*
- ✓ *Создание системы защиты файлового хранилища.*
- ✓ *Защищенный документооборот с разграничением прав доступа на уровне департаментов, проектов.*
- ✓ *Предоставление удаленного доступа к данным комплекса защищенно с мобильных устройств.*
- ✓ *Построение единого информационного портала по информационной безопасности - системы сбора, консолидации, хранения данных в защищенном виде с поддержкой хранения истории изменения файлов и возможностью безопасного совместного доступа к ним должностных лиц компании Россети.*

ЛИЦЕНЗИИ ATLANSYS SOFTWARE

Лицензии ФСБ:

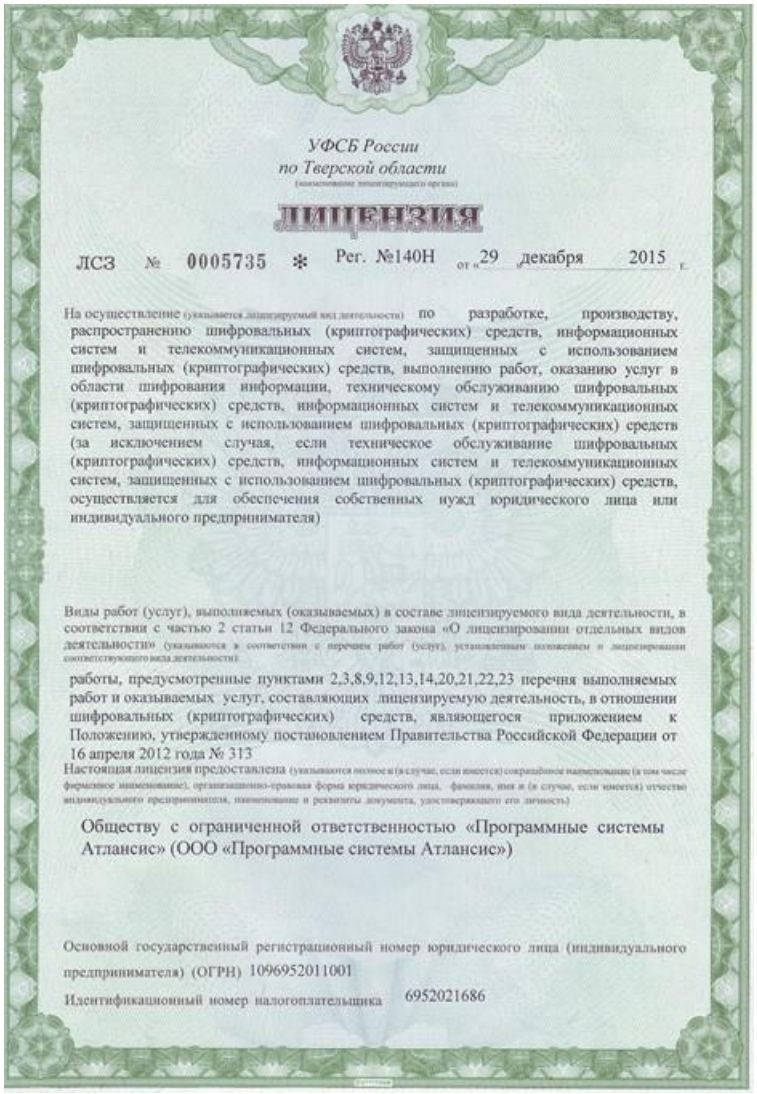
- ✓ *На осуществление работ с использованием сведений составляющих государственную тайну №1324.*
- ✓ *На деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем , защищенных с использованием шифровальных (криптографических) средств №140Н от 29 декабря 2015 года.*

Лицензии ФСТЭК:

- ✓ *На деятельность по технической защите конфиденциальной информации №2789 от 15 января 2016 года.*
- ✓ *На деятельность по разработке и производству средств защиты конфиденциальной информации №1501 от 15 января 2016 года.*

Государственная аккредитация организаций Министерством связи и массовых коммуникаций Российской Федерации, осуществляющих деятельность в области информационных технологий (№5175).

Сертификат системы контроля качества в соответствие со стандартом ГОСТ ISO 9001, ГОСТ ISO 27001.



УФСБ России
по Тверской области

ЛИЦЕНЗИЯ

ЛСЗ № 0005735 Рег. №140Н от «29» декабря 2015 г.

На осуществление по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, выполнению работ, оказанию услуг в области шифрования информации, техническому обслуживанию шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств (за исключением случая, если техническое обслуживание шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) средств, осуществляется для обеспечения собственных нужд юридического лица или индивидуального предпринимателя)

работы, предусмотренные пунктами 2,3,8,9,12,13,14,20,21,22,23 перечня выполняемых работ и оказываемых услуг, составляющих лицензируемую деятельность, в отношении шифровальных (криптографических) средств, являющегося приложением к Положению, утвержденному постановлением Правительства Российской Федерации от 16 апреля 2012 года № 313

Обществу с ограниченной ответственностью «Программные системы Атлансис» (ООО «Программные системы Атлансис»)

Основной государственный регистрационный номер юридического лица (индивидуального предпринимателя) (ОГРН) 1096952011001

Идентификационный номер налогоплательщика 6952021686

129327, Москва, ул. Коминтерна, д. 7, корпус 2,
офисы 300/9, 300/13

Телефон: +7 (495) 470-09-92

Сайт компании: www.atlansys.ru
Email: info@atlansys.ru

Atlansys Software

Atlansys WHITECLOUD