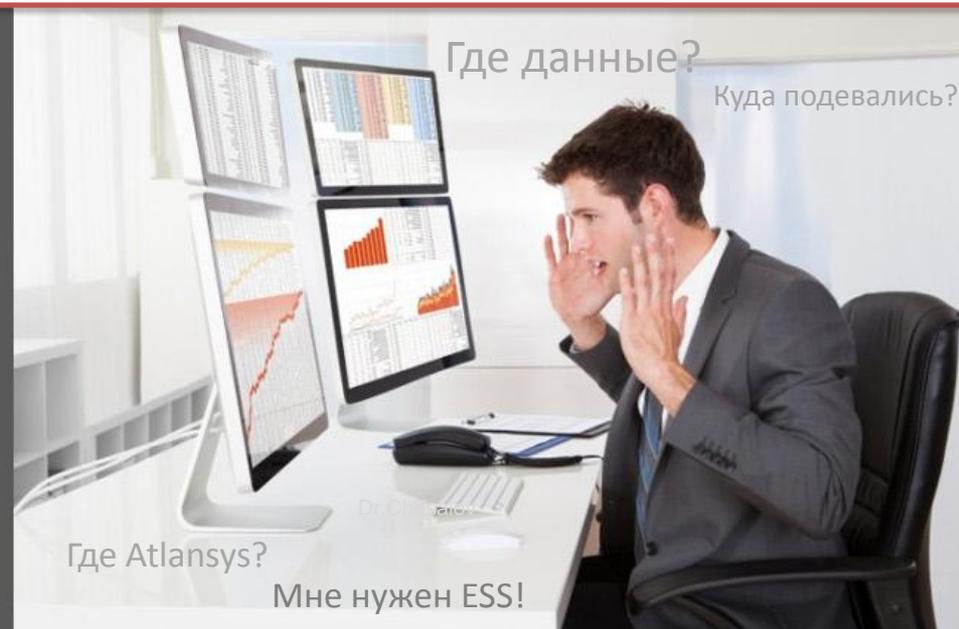


Atlansys ESS

Решение №1

по защите персональных данных и
коммерческой тайны
на АРМ, серверах и системах
хранения данных

Сертифицировано ФСБ РФ



БЕЗОПАСНОСТЬ И РАЗВИТИЕ

Передовые технологии и интеграция
в СУИБ

Шифрование данных на серверах и
ПЭВМ

Контроль средств хранения данных и
внешних носителей

Централизованное управление

РЕГУЛЯТОРЫ

Соответствует требованиям
российского и зарубежного
законодательства

ФЗ №152 «О персональных данных»

ФЗ №98 «О коммерческой тайне»

СТО БР ИББС-1.0-2010

ISO/IEC 27001:2005

ТЕХПОДДЕРЖКА

Решение задач по разработке систем
ИБ любой сложности

Разработка решений под конкретного
заказчика

Интеграция

Техническая поддержка 7x24

Atlansys Enterprise Security System

СИСТЕМА ЗАЩИТЫ КОРПОРАТИВНЫХ ДАННЫХ

ЗАЧЕМ И ДЛЯ ЧЕГО?

ЧТО МОЖЕТ ATLANSYS ESS ?

ATLANSYS ESS И СУИБ.
УПРАВЛЕНИЕ РИСКАМИ.
КОНФИДЕНЦИАЛЬНОСТЬ,
ЦЕЛОСТНОСТЬ И
ДОСТУПНОСТЬ

ТРЕБОВАНИЯ
РЕГУЛЯТОРОВ



Atlansys Enterprise Security System

ЗАЧЕМ И ДЛЯ ЧЕГО?

- Atlansys ESS - надежная защита персональных данных и коммерческой тайны на корпоративных серверах и рабочих станциях от внешних и внутренних угроз.
- Atlansys ESS необходимое решение при формировании корпоративной системы управления информационной безопасностью (СУИБ).
- Atlansys ESS соответствует «Требованиям к шифровальным криптографическим средствам , предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» и «Требованиям к средствам электронной подписи» по классам КС1/КС2.
- Снижение стоимости владения на ИТ инфраструктуру + Техническая поддержка, бесплатные обновления системы и доработка решения под индивидуальные требования заказчика – гарантированный положительный результат.
- Повышение управляемости и защищенности бизнеса.
- Выполнение требований регуляторов. Соответствие отечественному и международному законодательству и стандартам.

Atlansys Enterprise Security System

ЗАЧЕМ И ДЛЯ ЧЕГО?

- Безопасность файловых серверов. Шифрование разделов дисков с общими файлами и документами пользователей.
- Безопасность почтовых серверов. Шифрование раздела жесткого диска, на котором находится хранилище электронных сообщений.
- Безопасность серверов баз данных. Шифрование раздела жесткого диска, на котором находится бухгалтерские, финансовые, информационно-справочные и другие базы данных.
- Безопасность серверов приложений. Шифрование раздела жесткого диска, на котором находится критичные приложения для обеспечения ключевых бизнес-процессов.
- Безопасность систем хранения данных и систем сетевого хранения данных в сетях SAN.
- Безопасность рабочих станций, ноутбуков и сменных носителей информации.

Atlansys Enterprise Security System

ЧТО МОЖЕТ ATLANSYS ESS?

- **Интегрироваться в корпоративную систему управления информационной безопасностью. Поддержка технологии PKI (Public Key Infrastructure), различных криптопровайдеров (Microsoft, Crypto Pro и т.д.) и т.д.**
- **Шифровать данные на серверах, рабочих станциях, ноутбуках и сменных носителях информации.**
- **Централизованно управлять пользователями и их профилями. Поддержка технологий MS Active Directory.**
- **Управлять ключами шифрования. Восстанавливать ключи и данные пользователей.**
- **Осуществлять контроль средств хранения данных и сменных носителей. Черные и белые списки устройств хранения.**
- **Протоколировать события информационной безопасности.**
- **Гарантированно удалять ненужные данные под контролем администратора.**

Atlansys Enterprise Security System

УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Источник угроз	Пример воздействия угрозы	Контрмеры, реализуемые с помощью Atlansys ESS
Злоумышленник, получивший физический доступ к персональному компьютеру (дискам с конфиденциальными данными) и обладающий возможностью привлечения вычислительных ресурсов для получения доступа к данным.	Персональный компьютер целиком или только носители с конфиденциальной информацией были похищены с целью извлечения информации. Мобильный компьютер был утерян или украден во время выездной работы сотрудника.	Криптографическая защита данных на жестких и съемных дисках методом их «прозрачного» шифрования. Данные на защищенных дисках всегда хранятся в зашифрованном виде. Даже в случае изъятия или утери компьютера, данные невозможно использовать. Для криптографической защиты данных могут применяться стойкие алгоритмы шифрования (AES и ГОСТ 28147-89 с длиной ключа 256 бит и Blowfish с длиной ключа 448 бит); Регулярная смена ключа защищенного диска и/или алгоритма шифрования.
Постороннее лицо, получившее легальный доступ к серверу или рабочей станции (например, сервисное обслуживание)	Персональный компьютер (диск), содержащий конфиденциальные данные, был отправлен на ремонт в стороннюю организацию или в технический отдел.	Для смены ключа и/или алгоритма шифрования не требуется сначала расшифровывать данные и снимать с них защиту, а затем их зашифровывать с новым ключом и/или алгоритмом шифрования, благодаря чему в любой момент времени данные надежно защищены. Сетевой доступ к зашифрованным данным запрещен. Система защиты от сбоев гарантирует целостность данных при сбоях электропитания и в других нештатных ситуациях.
Стихийное бедствие (пожар, наводнение), проникновение в ИС, физическое проникновение чужих лиц в помещение	Экстренная эвакуация оборудования требует его выключения. Экстренное выключение, особенно во время выполнения операций шифрования может привести к нарушению целостности данных.	При возобновлении питания от сети приостановленный процесс автоматически продолжится. Вынос всех административных операций на уровень сервера управления исключает ошибку пользователя.

Atlansys Enterprise Security System

УПРАВЛЕНИЕ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Источник угроз	Пример воздействия угрозы	Контрмеры, реализуемые с помощью Atlansys ESS
«Любопытный» сотрудник	<p>Пользователь может получить доступ по сети к дискам другого персонального компьютера.</p> <p>Пользователь, работающий на компьютере общего пользования, имеет возможность получить доступ к файлам других пользователей данного компьютера.</p>	<p>Данные, обрабатываемые пользователями и хранящиеся на защищенных дисках, не доступны по сети.</p> <p>Доступ к защищенным дискам возможен только при наличии электронного ключа eToken и знания пароля.</p>
Администратор домена Windows	<p>Администратор домена Windows имеет неограниченный доступ ко всем компьютерам домена, в том числе к содержимому их дисков по сети через административные сетевые ресурсы и в режиме удаленного рабочего стола.</p>	<p>Atlansys ESS запрещает прямой сетевой доступ к защищенным дискам даже для администратора домена через административные сетевые ресурсы.</p>

Atlansys Enterprise Security System

КОНФИДЕНЦИАЛЬНОСТЬ, ЦЕЛОСТНОСТЬ И ДОСТУПНОСТЬ

- **Конфиденциальность данных:**
 - Реализована поддержка технологии открытых ключей PKI (Public Key Infrastructure).
 - Реализована поддержка различных криптопровайдеров (Microsoft, Crypto Pro и т.д.).
 - Реализовано шифрование данных различными алгоритмами (ГОСТ 28147-89, AES, Blowfish).
 - Гарантированным уничтожением устаревших данных (стандарты ГОСТ, DoD, NAVSO).
 - Поддержкой аппаратных ключей (eToken Pro, смарт-карта).

- **Целостность данных:**
 - Поддержкой целостности модулей самого приложения и заголовков криптообъектов.
 - Защитой от программных и аппаратных сбоев во время выполнения криптографических операций, включая перебои с электропитанием.
 - Поддержкой различных систем резервного копирования данных.

- **Доступность данных:**
 - Поддержкой MS Active Directory.
 - Поддержкой фонового режима выполнения криптографических операций, не требующего прекращения работы пользователя.
 - Функцией смены пароля и списка сертификатов на криптообъектах.
 - Функцией восстановления ключей пользователей из хранилища ключей на ЦУ.

- **Подлинность данных:**
 - Реализованы технологии электронно-цифровой подписи.
 - Обеспечение защиты хранимых на серверах ключей.

Atlansys Enterprise Security System

ТРЕБОВАНИЯ ЗАКОНОДАТЕЛЬСТВА И РЕГУЛЯТОРОВ

- Atlansys ESS соответствует «Требованиям к шифровальным криптографическим средствам, предназначенным для защиты информации, не содержащей сведений, составляющих государственную тайну» и «Требованиям к средствам электронной подписи» по классам КС1/КС2.
- **Федеральные законы и стандарты РФ:**
 - ФЗ №152 «О персональных данных».
 - ФЗ №98 «О коммерческой тайне».
 - Стандарт банка России СТО БР ИББС-1.0-2010.
- **Международные законы и стандарты:**
 - Требования к финансовой отчетности по закону Sarbanes-Oxley (SOX). IT Control Objectives for SOX.
 - Стандарт безопасности платежных карт PCI DSS.
 - Международный стандарт безопасности ISO/IEC 27001:2005.



Atlansys Enterprise Security System

НАШИ ПРОЕКТЫ

- На сегодняшний день, более 10 000 организаций и Предприятий различных сфер деятельности используют при защите своих корпоративных серверов и рабочих станций решение Atlansys ESS



Защищено: 12 000 рабочих мест



Защищено: 7 500 рабочих мест



Защищено: 4 000 рабочих мест



БАШНЕФТЬ
АКЦИОНЕРНАЯ НЕФТЯНАЯ КОМПАНИЯ

Защищено: 2 000 рабочих мест

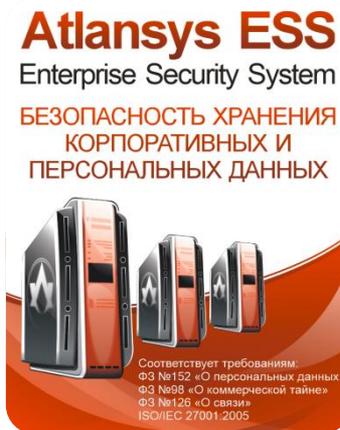


РОССЕТИ

Защищено: 1 000 рабочих мест



Защищено: 8 000 АРМ



Atlansys Enterprise Security System

НАШИ ЛИЦЕНЗИИ

Лицензии ФСБ:

- На осуществление работ с использованием сведений составляющих государственную тайну №1324.
- На деятельность по разработке, производству шифровальных (криптографических) средств №10050п.
- На деятельность по техническому обслуживанию шифровальных (криптографических) средств №69х.
- На деятельность по распространению шифровальных (криптографических) средств №69р.



Лицензии ФСТЭК:

- На деятельность по технической защите конфиденциальной информации №1220.
- На деятельность по разработке и производству средств защиты конфиденциальной информации №0726.



Не ищите компромиссов

Мы с Вами 10 лет !

- ✓ Atlansys WhiteCloud – лучшее решение 2013
- ✓ Atlansys ESS – лучшее решение 2008 – 2010
- ✓ Atlansys Bastion Pro – лучшее решение 2008 - 2009



Наши контакты

129327, Москва, ул. Коминтерна, д. 7,
корпус 2, офис 300/11

Телефон: +7 (495) 470-09-92

Сайт компании: www.atlansys.ru
E-mail: info@atlansys.ru

Отдел продаж

Телефон: +7 (495) 470-09-92
E-mail: sales@atlansys.ru

Техническая поддержка

Телефон: +7 (495) 470-09-92
E-mail: support@atlansys.ru