

 Atlansys Software

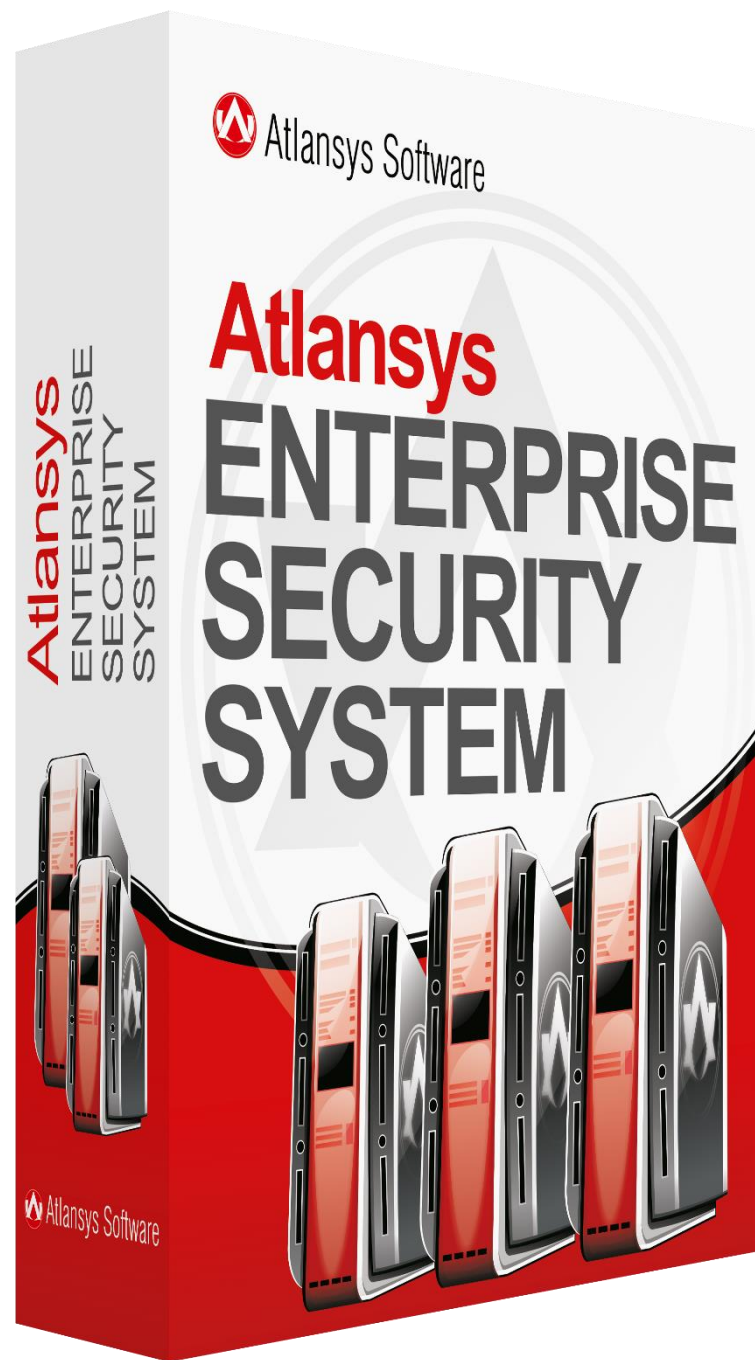
Atlansys ENTERPRISE SECURITY SYSTEM



ATLANSYS ENTERPRISE SECURITY SYSTEM

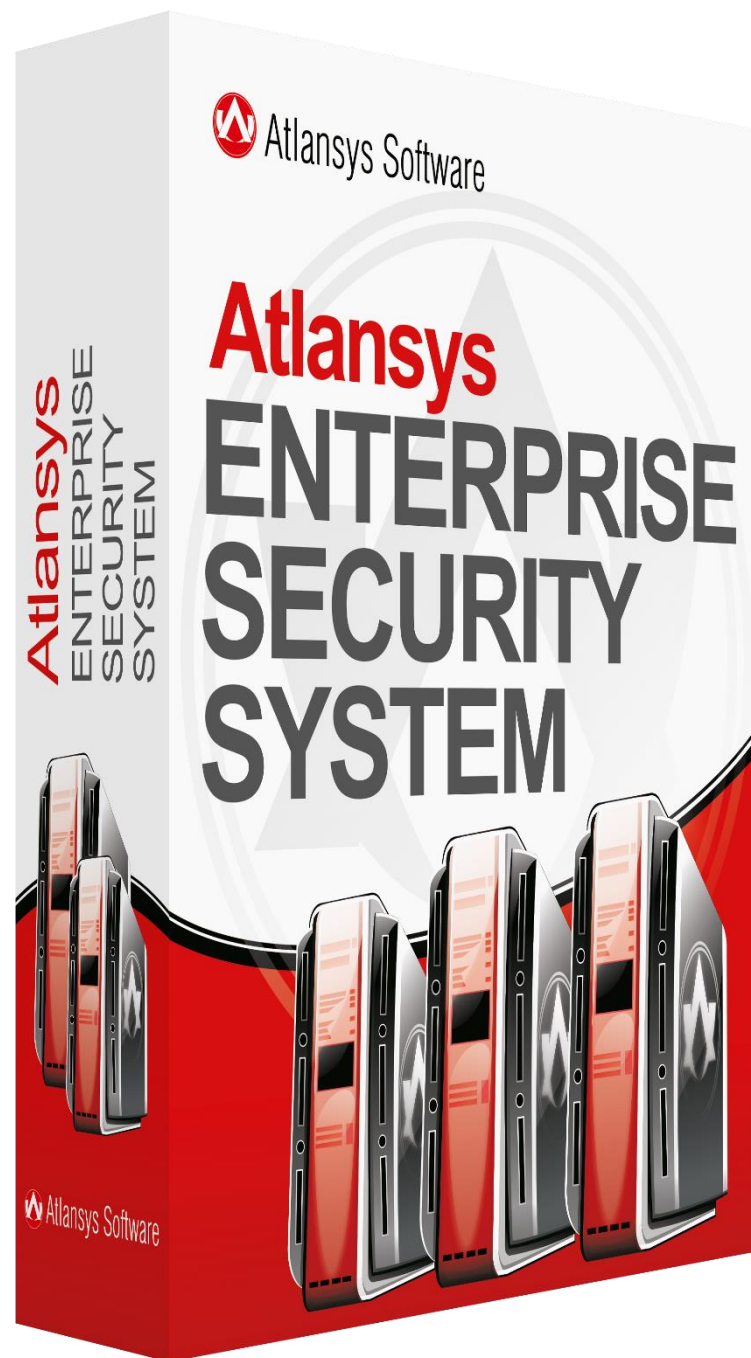
Atlansys Enterprise Security System - **корпоративная система**, обеспечивающая комплексную защиту конфиденциальной информации на рабочих станциях, ноутбуках, серверах, системах хранения данных и внешних носителях информации.

- ✓ **Защита ИСПДн с уровнем защищенности ПДн 4УЗ, 3УЗ, 2УЗ**
- ✓ **Защита документов при передаче по открытым каналам связи**
- ✓ **Контроль внешних носителей** в компании:
 - ✓ Правила пользования (блокировка носителей; подключение носителей в режиме чтения; в режиме чтения/записи);
 - ✓ Логирование действий пользователей над файлами, расположенными на внешних носителях;
 - ✓ «Черный» и «белый» списки внешних носителей;
 - ✓ Теневое копирование;
 - ✓ Определение и контроль зашифрованных носителей.



ATLANSYS ENTERPRISE SECURITY SYSTEM

- ✓ **Защита от несанкционированного доступа** к корпоративным ресурсам компании со стороны нарушителя.
- ✓ **Шифрование ноутбуков** (системный раздел, логические диски с базами данных).
- ✓ **Создание/проверка электронной подписи** документов по стандарту ГОСТ.
- ✓ **Централизованное управление** защищенными ресурсами и восстановление доступа к ним при утере сертификата или пароля пользователя.
- ✓ **Защита файловых и почтовых серверов**, серверов приложений и файлов баз данных.
- ✓ **Защита локальных почтовых хранилищ** на рабочих станциях и хранилища MS Exchange.
- ✓ **Гарантированное уничтожение выбранных данных** по средствам алгоритма ГОСТ.



ATLANSYS

ENTERPRISE SECURITY SYSTEM

Конфиденциальность данных осуществляется:

- ✓ Поддержкой технологии открытых ключей PKI (Public Key Infrastructure)
- ✓ Поддержкой различных криптопровайдеров (Microsoft, Крипто ПРО и др.)
- ✓ Шифрованием данных различными алгоритмами (ГОСТ, AES, Blowfish)
- ✓ Гарантированным уничтожением устаревших данных по стандарту ГОСТ
- ✓ Поддержкой аппаратных ключевых носителей (eToken, ruToken, JaCarta и др.)

Целостность данных осуществляется:

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

Доступность данных осуществляется:

- ✓ Поддержкой службы каталогов 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 на ЦУ

Подлинность данных осуществляется:

- ✓ Поддержкой технологии электронной подписи документов (ЭП)
- ✓ По средствам обеспечения защиты хранимых на серверах ключей

АРХИТЕКТУРА ATLANSYS ENTERPRISE SECURITY SYSTEM

Atlansys ESS состоит из трех компонентов:

- ✓ Центр Управления Atlansys ESS (в дальнейшем ЦУ)
- ✓ Криптосервер Atlansys ESS (защита корпоративных серверов)
- ✓ Клиент Atlansys ESS (защита рабочих станций и ноутбуков)

Защищенный Сервер



Сервер безопасности на базе Atlansys ESS



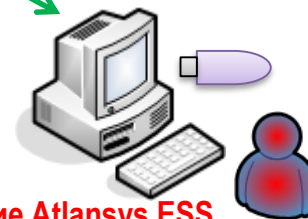
**Контролеры Домена
(Active Directory DC's)
Удостоверяющий Центр
Сертификации PKI**

Криптосервер Atlansys ESS

Защита данных на жестких дисках
Защита резервных копий
Гарантированное уничтожение данных
Режим экстренного выключения системы
Запуск внешних скриптов после открытия и перед закрытием криптообъектов
Поддержка Active Directory

Центр управления Atlansys ESS

Восстановление, смена ключей пользователей и серверов
Централизованное управление криптообъектами и их политиками безопасности в Atlansys ESS
Централизованный контроль внешних носителей
Гибкая система протоколирования событий пользователей
Возможность работы с открытыми ключами и размещения их на электронных носителях (eToken, ruToken, JaCarta)



Удаленное управление Atlansys ESS

Консоль Центра управления

Создание политик использования Atlansys ESS
Восстановление ключей пользователей
Управление защищенными серверами
Удаленная установка Atlansys ESS

Клиент Atlansys ESS

Шифрование жестких дисков и внешних накопителей
Создание зашифрованных контейнеров
Шифрование и сжатие данных при передаче по электронной почте или через Интернет
Гарантированное удаление данных
Режим экстренного выключения системы
Электронная Подпись (ЭП) документов

**Защищенные рабочие
станции и ноутбуки**



АРХИТЕКТУРА ATLANSYS ENTERPRISE SECURITY SYSTEM

Основные возможности ЦУ:

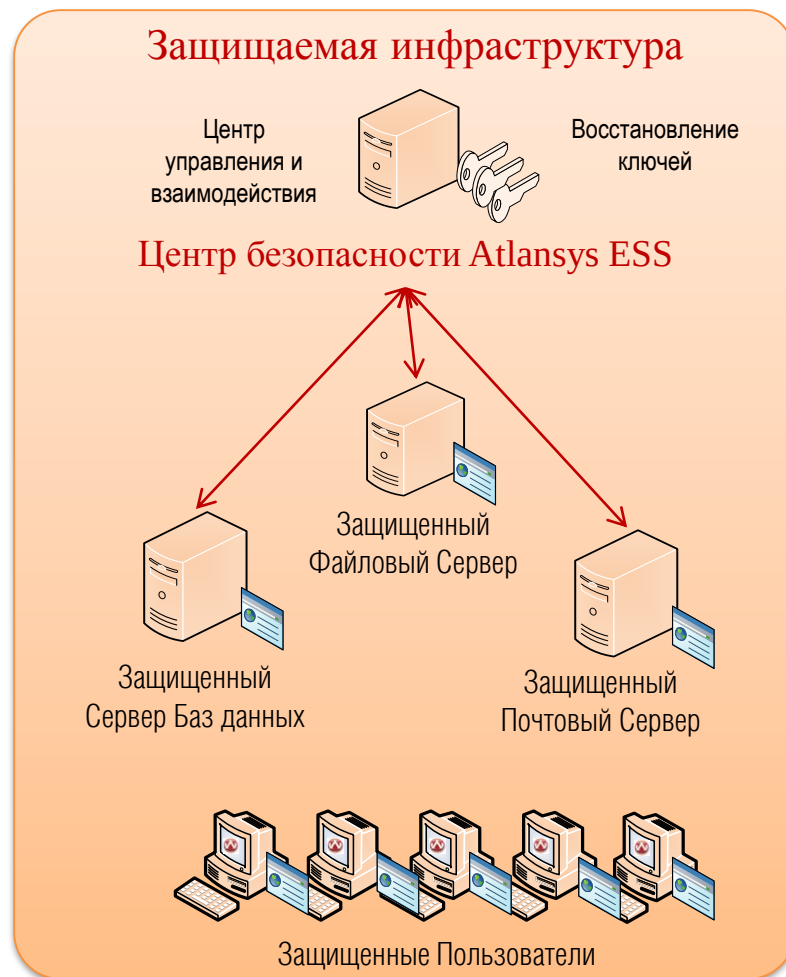
- ✓ Интеграция с MS Active Directory и поддержка удостоверяющих центров организации
- ✓ Централизованное выполнение политик Красной кнопки «Тревоги»
- ✓ Централизованное развертывание системы на рабочие станции пользователей
- ✓ Высокая надежность системы (>10 тысяч пользователей на один Центр управления (сервер)).

Основные функции Консоли ЦУ:

- ✓ Удаленное управление криптообъектами пользователей
- ✓ Восстановление ключей пользователей
- ✓ Полный контроль внешних носителей и действий пользователей в организации

Основные криптообъекты:

- ✓ Криптодиск, Криптоконтейнер, Автономный криптофлэш диск, Криптоархив и Автономный криптоархив.



ФУНКЦИОНАЛ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ХРАНЕНИИ

Хранение КТ и ПДн на компьютере или внешних носителях



Криптодиск – это полностью зашифрованный диск компьютера или внешний USB накопитель

Назначение:

Хранение больших объемов конфиденциальной информации



Криптоконтейнер – это зашифрованный файл на компьютере, который отображается в виде диска операционной системы

Назначение:

Хранение Небольших объемов конфиденциальной информации



Автономный криптофлэш диск – это полностью зашифрованное съемное устройство (обычно это USB-flash накопитель), с которым можно работать, не имея установленного на компьютере клиента Atlansys ESS

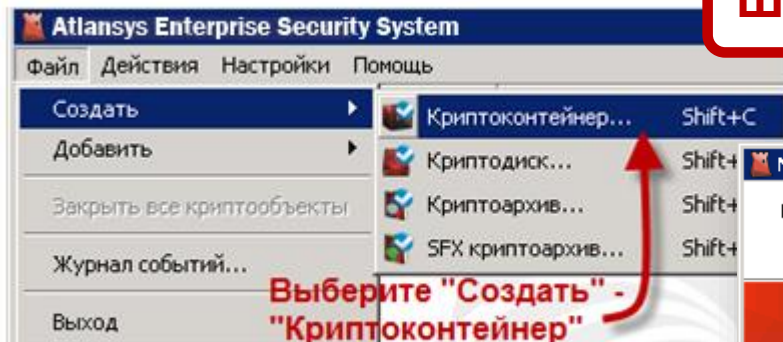
Назначение: Хранение конфиденциальной информации на внешних носителях автономно

- Криптодиск и криптоконтейнер неотличимы от обычных дисков операционной системы
- Процесс шифрования и дешифрования информации производится автоматически и прозрачен для пользователя, при этом производительность компьютера практически не снижается

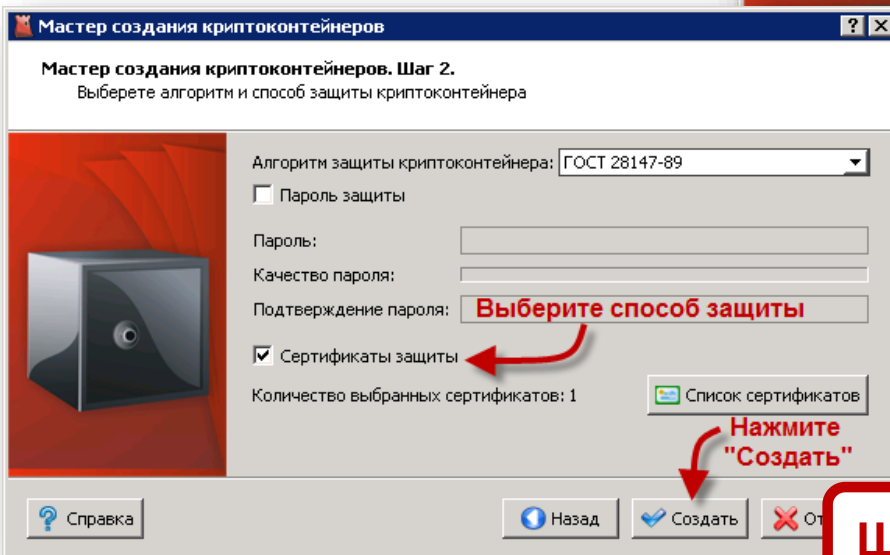
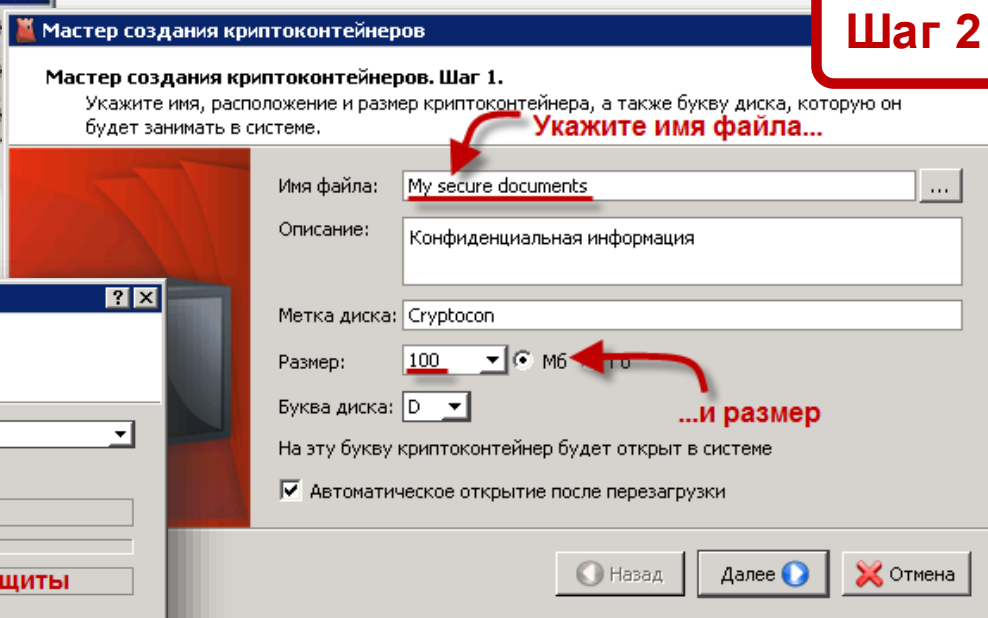
СОЗДАНИЕ КРИПТОКОНТЕЙНЕРА

Аналогично создание криптодиска

Шаг 1



Шаг 2



Шаг 3

УГРОЗЫ БЕЗОПАСНОСТИ USB-НАКОПИТЕЛЕЙ В ОРГАНИЗАЦИИ

Следствие универсальности, мобильности и компактности:

- кража/потеря
- вынос за пределы охраняемой зоны
- внедрение ложного носителя

Угрозы информации и ИС

- нарушение конфиденциальности и целостности информации на USB-носителе
- навязывание ложной информации
- вредоносное ПО (рекламное ПО, шпионские программы, вирусы, черви, троянские программы, руткиты, эксплойты и др.)

СОЗДАНИЕ АВТОНОМНОГО КРИПТОФЛЭШ ДИСКА

Шаг 1

Atlansys ESS - Навигатор

Файл Действия Настройки Помощь

- Создать
 - Криптоконтейнер... Shift+C
 - Криптодиск... Shift+D
 - Автономный криптофлэш диск...
- Добавить
- Шифровать
- Заккрыть все криптообъекты
- Активировать красную кнопку
- Журнал событий...
- Выход

Шаг 2

Мастер создания автономного криптофлэш диска

Мастер создания автономного криптофлэш диска. Шаг 1.
Выберите том для создания автономного криптофлэш диска.

Буква	Метка	Тип тома	Диск	Раздел	Файловая система	Размер
...	...	Основной	2	1	FAT32	101,00 МБ...

Шаг 3

Мастер создания автономного криптофлэш диска

Мастер создания автономного криптофлэш диска. Шаг 2.
Выберите тип защиты криптофлэш диска.

Алгоритм защиты: ГОСТ 28147-89

☐ Защита паролем

Пароль:

Качество пароля:

Подтверждение пароля:

☒ Защита сертификатами

Количество выбранных сертификатов: 1 [Список сертификатов](#)

[Назад](#) [Создать](#) [Отмена](#)

[Справка](#) [Далее](#) [Отмена](#)

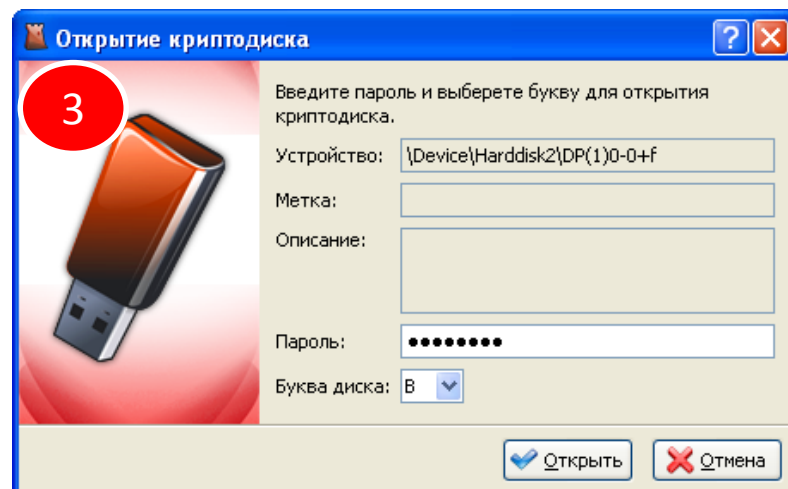
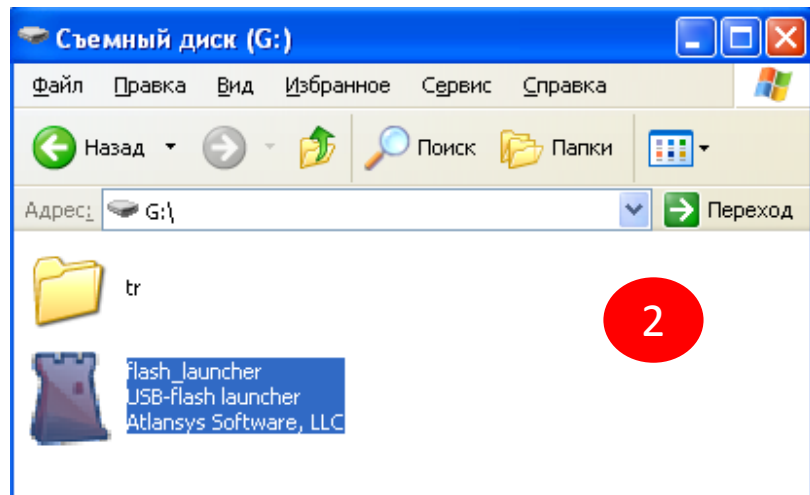
РАБОТА С АВТОНОМНЫМ КРИПТОФЛЭШ ДИСКОМ

После успешного создания закрытого криптофлэш диска в системе, на флэшке появится два раздела, первый - открытый раздел размером 256 Мб, где размещается мини-клиент для открытия второй защищенной области, занимающей оставшееся место флэшки.

Запуск мини-клиента на флэш диске вызовет стандартный диалог открытия криптодисков, такой же, как в навигаторе Atlansys ESS, в котором потребуется указать пароль или сертификат, а также выбрать букву (при желании), под которой защищенный раздел криптофлэш диска будет отображаться в системе.

Устройства со съемными носителями

Диск 3,5 (A:)	1	Диск 3,5
DVD-дисковод (E:)		CD-дисковод
CD-дисковод (F:)		CD-дисковод
Съемный диск (G:)		Съемный диск



Жесткие диски

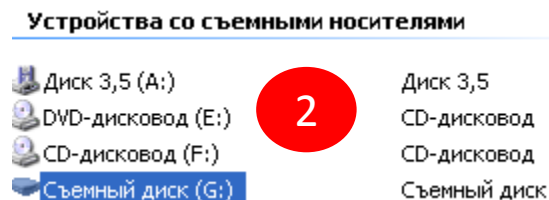
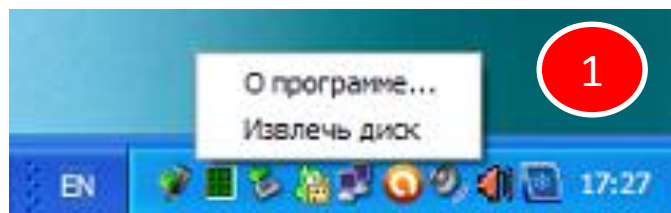
Локальный диск (B:)	4	Локальный диск	66,2 МБ	66,2 МБ
Локальный диск (C:)		Локальный диск	149 ГБ	133 ГБ
Work (D:)		Локальный диск	232 ГБ	228 ГБ

РАБОТА С АВТОНОМНЫМ КРИПТОФЛЭШ ДИСКОМ

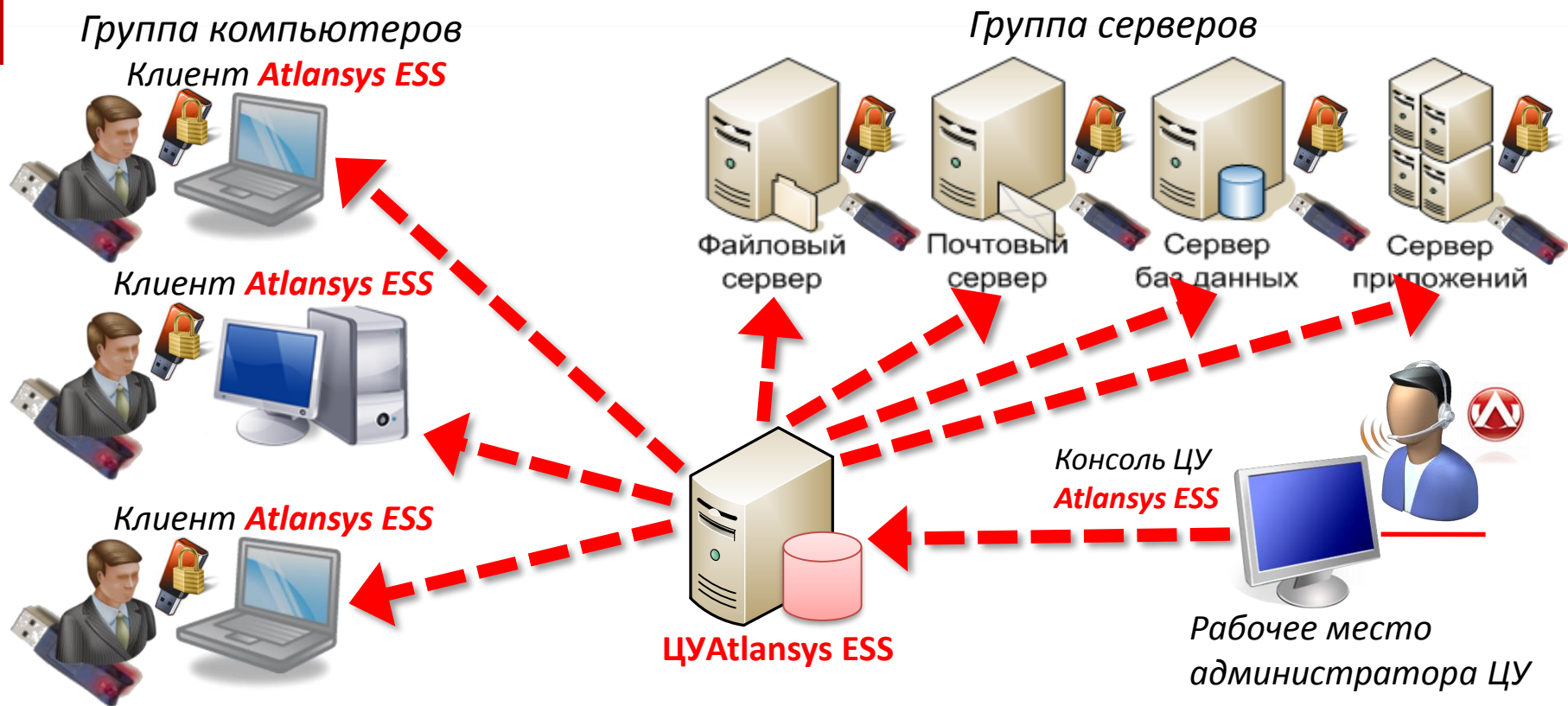
После успешного открытия, в системе появится новый диск, открытый на ранее выбранную букву, с которым можно работать, как с любым обычным диском операционной системы.

Чтобы закрыть защищенный раздел, следует выбрать пункт в контекстном меню программы в системном трее «Извлечь диск».

После этого буква защищенного раздела в операционной системе исчезнет, а открытый раздел криптофлэш диска снова станет доступен. Далее для извлечения устройства необходимо воспользоваться стандартным механизмом операционной системы.



КОНТРОЛЬ ВНЕШНИХ НОСИТЕЛЕЙ



- Централизованно Администратором ЦУ с консоли задается в свойствах группы компьютеров и группы серверов какой контроль внешних носителей будет применяться:



- Разрешить использовать криптофлэш диски
 - ✓ Только «на чтение»
 - ✓ Полный доступ к данным
- Запретить использовать криптофлэш диски



- Разрешить использовать внешние носители
 - ✓ Только «на чтение»
 - ✓ Полный доступ
- Запретить использовать внешние носители
- Использование «черных» и «белых» списков
- Теневое копирование

ФУНКЦИОНАЛ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ ПО ОТКРЫТЫМ КАНАЛАМ СВЯЗИ

Обмен КТ и ПДн между сотрудниками и контрагентами



Криптоархив – это сжатый зашифрованный файл, содержащий документы пользователя для передачи, который открывается только с помощью сертификатов пользователей между которыми происходит обмен

Назначение:

Обмен конфиденциальной информацией между сотрудниками



Автономный криптоархив – это сжатый зашифрованный файл, который открывается только по паролю без установки ПО Atlansys на компьютер пользователя

Назначение:

Обмен конфиденциальной информацией между сотрудниками компании и контрагентами (в рамках NDA)

- SFX-криптоархив не требует наличия клиента Atlansys ESS на стороне получателя информации
- Криптоархивы можно передавать любым удобным способом (e-mail, CD-ROM, USB flash и т.д.)

СОЗДАНИЕ КРИПТОАРХИВА

Шаг 1

Адрес: C:\Documents and Settings\test\Мои документы\Конфиденци...

Имя

Правил внутреннего трудового распорядка
Применение дисциплинарного взыскания к ра...
Проведение закупок товаров и работ
РП-029-6 Изменение организационной структ...
РП-199-3 Утверждение и открытие финансир...
Кодекс э...
Кодекс э...
ПТ-001-2...
РП-002-3 Организация документооборота слу...
РП-002-3 Приложение 2 Бланк Служебной зап...
СТ-082-1 Требования к написанию и оформле...

Открыть
Проводник
Найти...
Atlansys Enterprise Security System ▶
Scan for Viruses...
Отправить
Вырезать
Копировать
Создать ярлык
Удалить
Переименовать
Свойства

Создать криптоархив...
Создать SFX-криптоархив...
Гарантированно удалить...

Шаг 2

Atlansys Enterprise Security System / Создание криптоархива

Создание криптоархива
Именованные файлы и каталогов, которые будут добавлены в криптоархив.

Имя криптоархива: C:\Documents and Settings\kumi\Мои документы\Конфиденциальные документы\Конфиденциальные документы.crg

Именованные файлы:

Название	Размер	Путь	Действия
Правила внутреннего трудо...	1,67 Мбайт	C:\Documents and Settings\kumi\Мои документы\Конфиденци...	Действие 1 Действие 2
Применение дисциплинарно...	1,89 Мбайт	C:\Documents and Settings\kumi\Мои документы\Конфиденци...	Действие 1 Действие 2
Проведение закупок товаро...	2,62 Мбайт	C:\Documents and Settings\kumi\Мои документы\Конфиденци...	Действие 1 Действие 2
РП-029-6 Изменение организ...	5,47 Мбайт	C:\Documents and Settings\kumi\Мои документы\Конфиденци...	Действие 1 Действие 2
РП-199-3 Утверждение и от...	6,13 Мбайт	C:\Documents and Settings\kumi\Мои документы\Конфиденци...	Действие 1 Действие 2
Кодекс этических норм.doc	185,00 Кбайт	C:\Documents and Settings\kumi\Мои документы\Конфиденци...	Действие 1 Действие 2
Кодекс этических норм1.doc	102,00 Кбайт	C:\Documents and Settings\kumi\Мои документы\Конфиденци...	Действие 1 Действие 2
РП-002-3 Организация доку...	361,50 Кбайт	C:\Documents and Settings\kumi\Мои документы\Конфиденци...	Действие 1 Действие 2
РП-002-3 Организация доку...	738,00 Кбайт	C:\Documents and Settings\kumi\Мои документы\Конфиденци...	Действие 1 Действие 2
РП-002-3 Приложение 2 Бла...	71,00 Кбайт	C:\Documents and Settings\kumi\Мои документы\Конфиденци...	Действие 1 Действие 2
СТ-082-1 Требования к напи...	931,00 Кбайт	C:\Documents and Settings\kumi\Мои документы\Конфиденци...	Действие 1 Действие 2

Добавить файл Добавить каталог ☐ Удалить исходные файлы/каталоги после создания криптоархива

Нажмите "Далее"

Далее Отмена Справка

СОЗДАНИЕ КРИПТОАРХИВА

Atlansys Enterprise Security System / Создание криптоархива

Шаг 3

Нажмите "Добавить сертификат"

Список сертификатов
Добавление сертификатов получателей криптоархива. Выбранные сертификаты будут использоваться для шифрования файлов криптоархива.

Личный сертификат: Mikhail V. Kurzin

Сертификаты получателей криптоархива:

Владелец	Поставщик	Действителен до	Действия
Пичугин Дмитрий Олегович	winsa	30.11.2011 15:20:05	

Найдите получателей информации

Нажмите "Добавить"

Добавление сертификата

Выбор сертификатов получателей криптоархива

Доверенные пользователи Поиск сертификатов

Параметр поиска: ФИО Пичугин* Поиск

символ звёздочка (*) заменяет все символы.

Владелец	Поставщик	Действителен до	Действия
☒ Пичугин Дмитри...	winsa	30.11.2011 15:20:05	

Шаг 4

Создание криптоархива

Добавление сертификатов получателей криптоархива. Выбранные сертификаты будут использоваться для шифрования файлов криптоархива.

Личный сертификат: Kurzin (wifi)

Сертификаты получателей криптоархива:

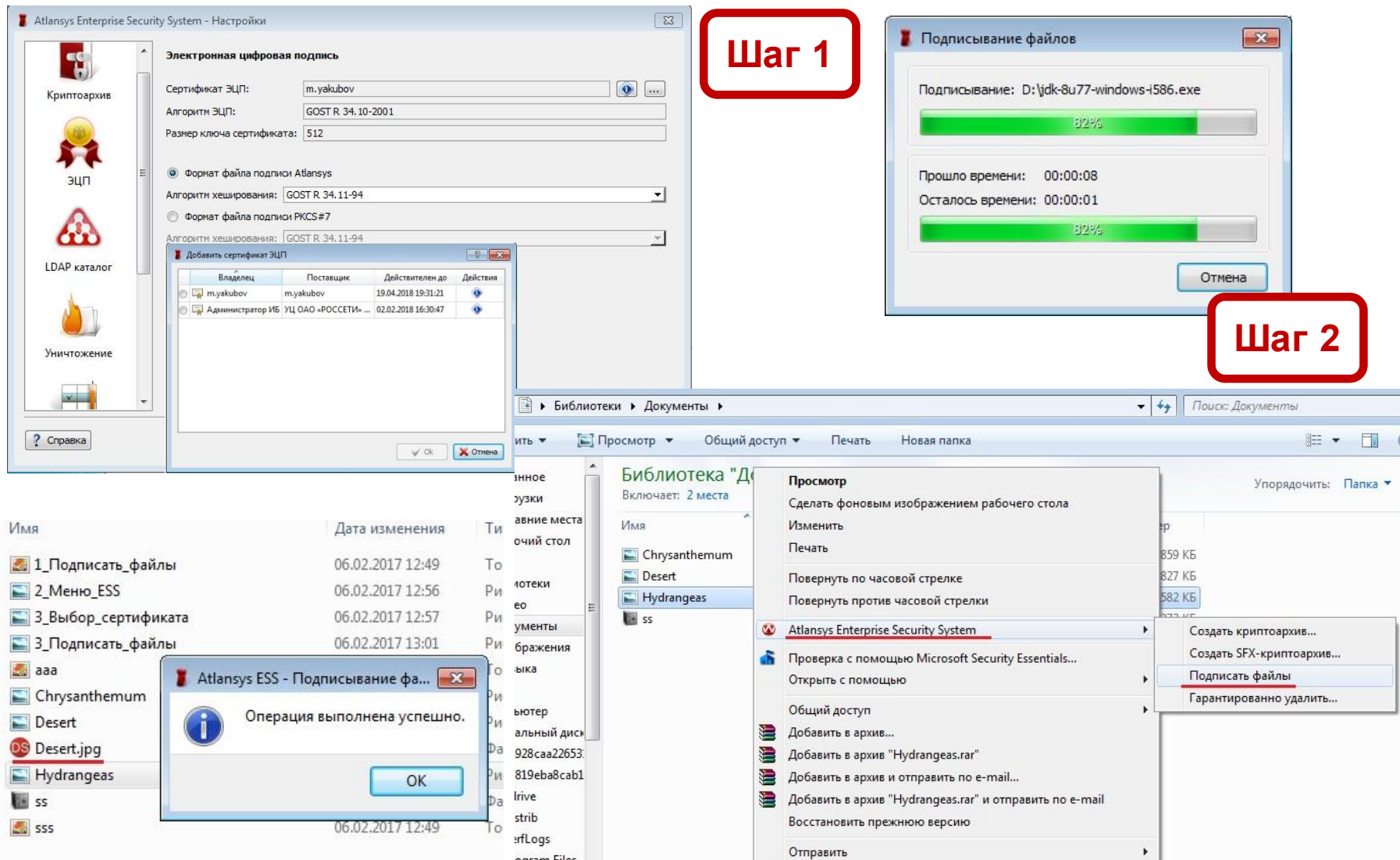
Владелец	Поставщик	Действителен до	Действия
	winsa	30.11.2011 15:20:05	

Нажмите "Создать"

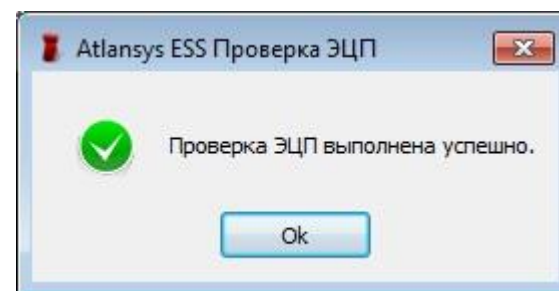
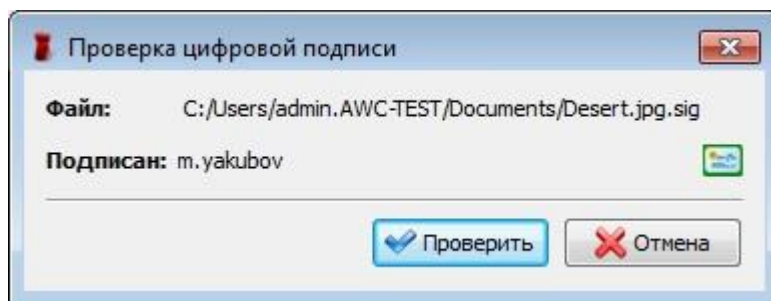
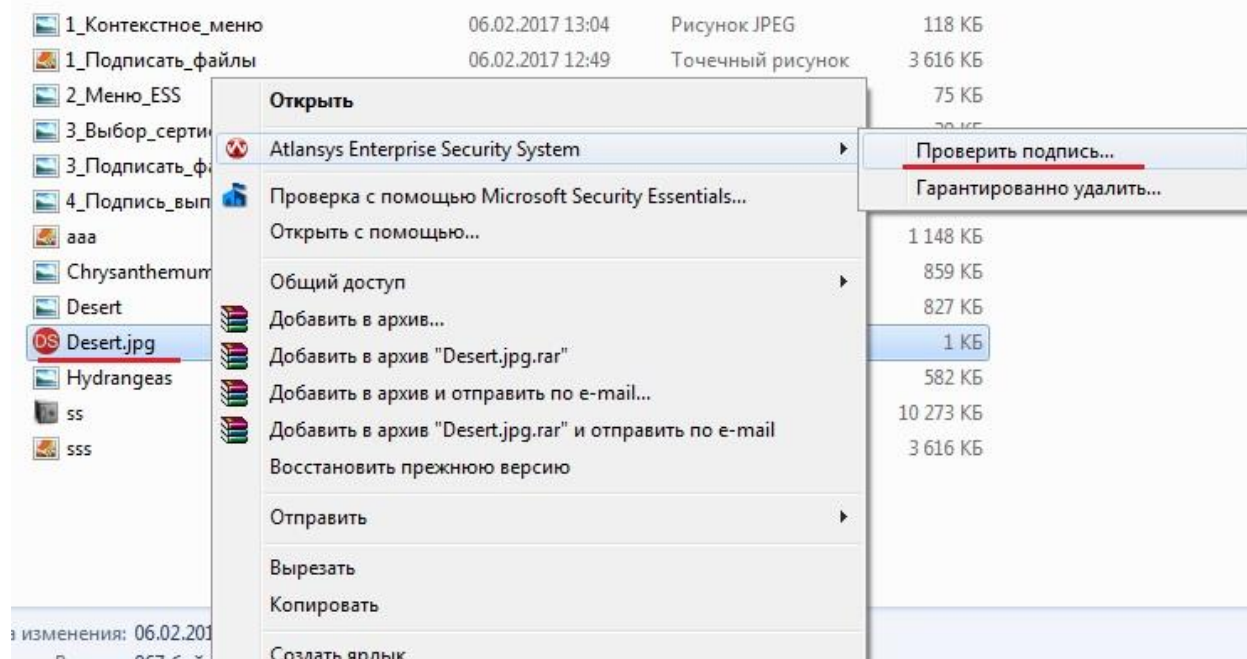
Добавить сертификаты

Назад Создать Отмена Справка

СОЗДАНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ



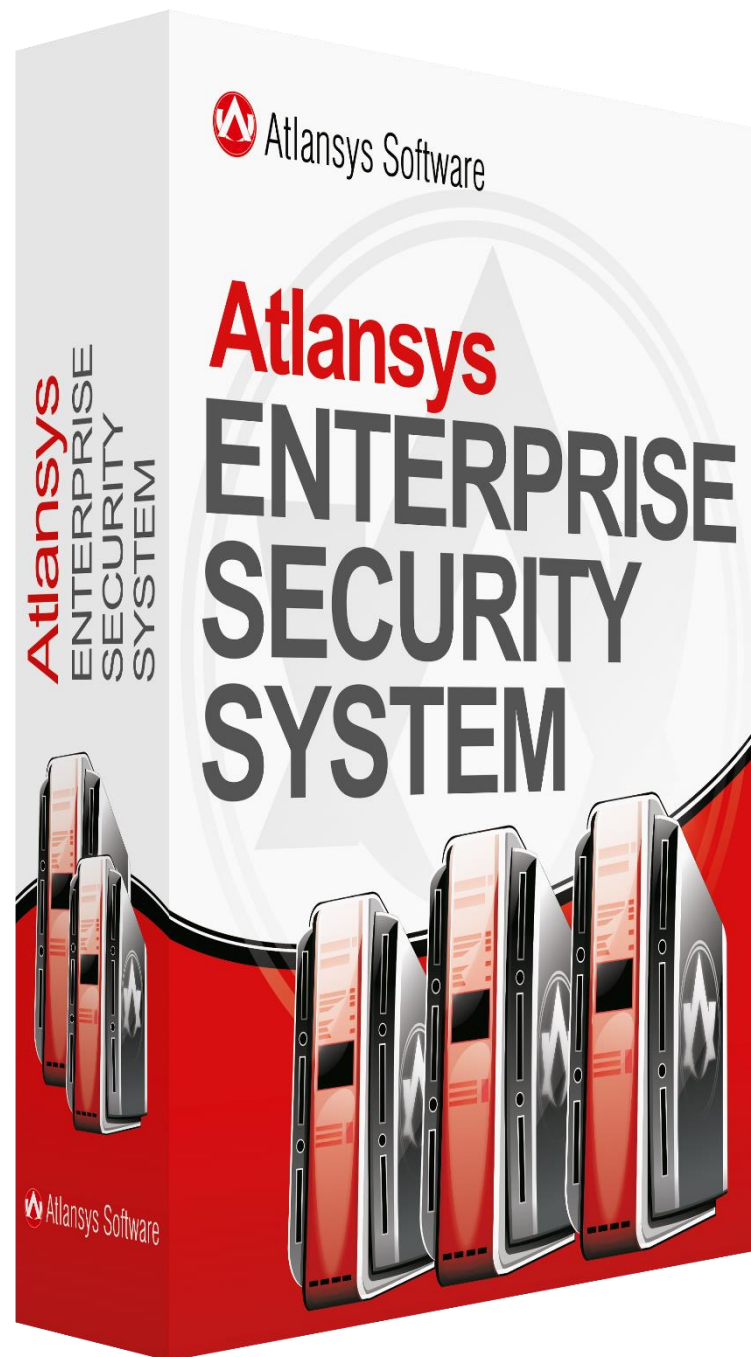
ПРОВЕРКА ЭЛЕКТРОННОЙ ПОДПИСИ



ПРЕИМУЩЕСТВА ATLANSYS ENTERPRISE SECURITY SYSTEM

Внедрение и использование Atlansys ESS позволит:

- ✓ Защитить персональные данные и коммерческую тайну от НСД.
- ✓ Снизить внутрикорпоративные риски ИБ в соответствии с законодательством РФ в части защиты информации.
- ✓ Реализовать полный контроль внешних носителей информации.
- ✓ Сотрудникам безопасно обмениваться конфиденциальной информацией по электронной почте как внутри защищенного периметра компании Заказчика так и за его пределами.
- ✓ Централизованно управлять защищенными ресурсами и доступом к ним, а также выполнять заданные групповые политики и процессы.
- ✓ Централизованно хранить ключи шифрования пользователей и восстанавливать доступ к корпоративным данным при их утере.
- ✓ Защитить территориально-распределенные корпоративные ресурсы компании Заказчика.



ATLANSYS ENTERPRISE SECURITY SYSTEM

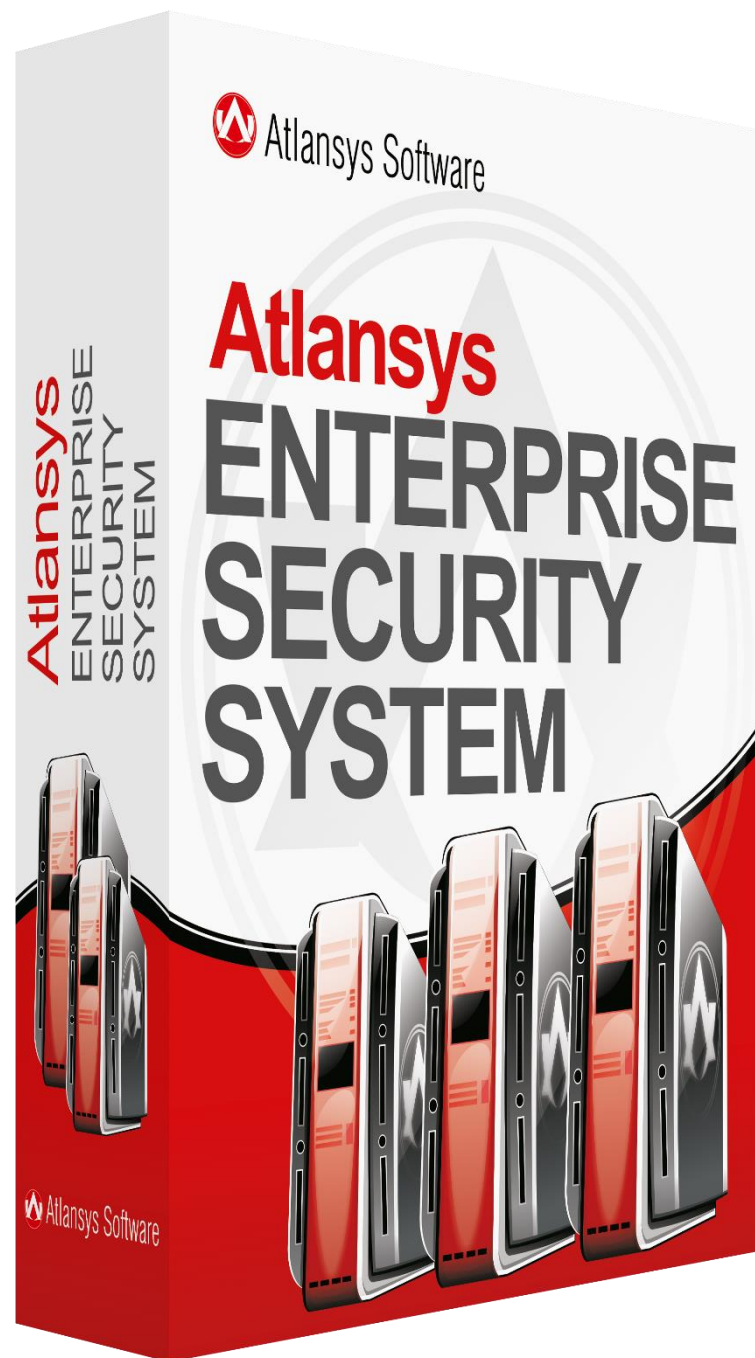
Atlansys ESS соответствует «Требованиям к шифровальным криптографическим средствам, предназначенным для защиты информации, не содержащей сведений, составляющих гос. тайну» и «Требованиям к средствам электронной подписи» по классам КС1/КС2.

Федеральные законы и стандарты РФ:

- ✓ ФЗ №152 «О персональных данных».
- ✓ ФЗ №98 «О коммерческой тайне».
- ✓ ГОСТ Р ИСО/МЭК 27001-2006.
- ✓ Стандарт Банка России СТО БР ИББС.
- ✓ Приказ ФСТЭК №21. Об Утверждении состава содержания организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн.

Международные законы и стандарты:

- ✓ Требования к финансовой отчетности по закону Sarbanes-Oxley (SOX).
- ✓ IT Control Objectives for SOX.
- ✓ Стандарт безопасности платежных карт PCI DSS.



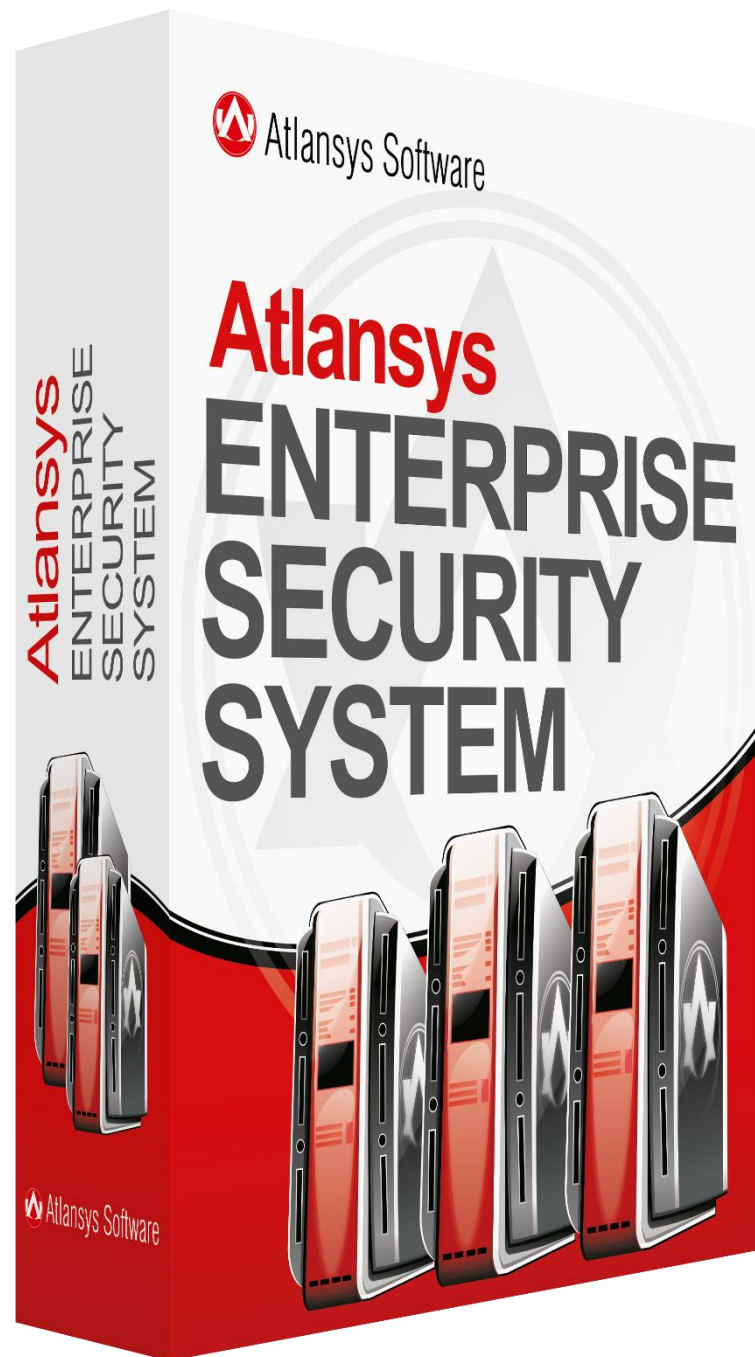
ATLANSYS ENTERPRISE SECURITY SYSTEM

Решение Atlansys Enterprise Security System

зарегистрировано в едином реестре российских программ для ЭВМ и баз данных №2030 от 08 октября 2016 года Приказом Минкомсвязи России от 07.10.2016 №487.

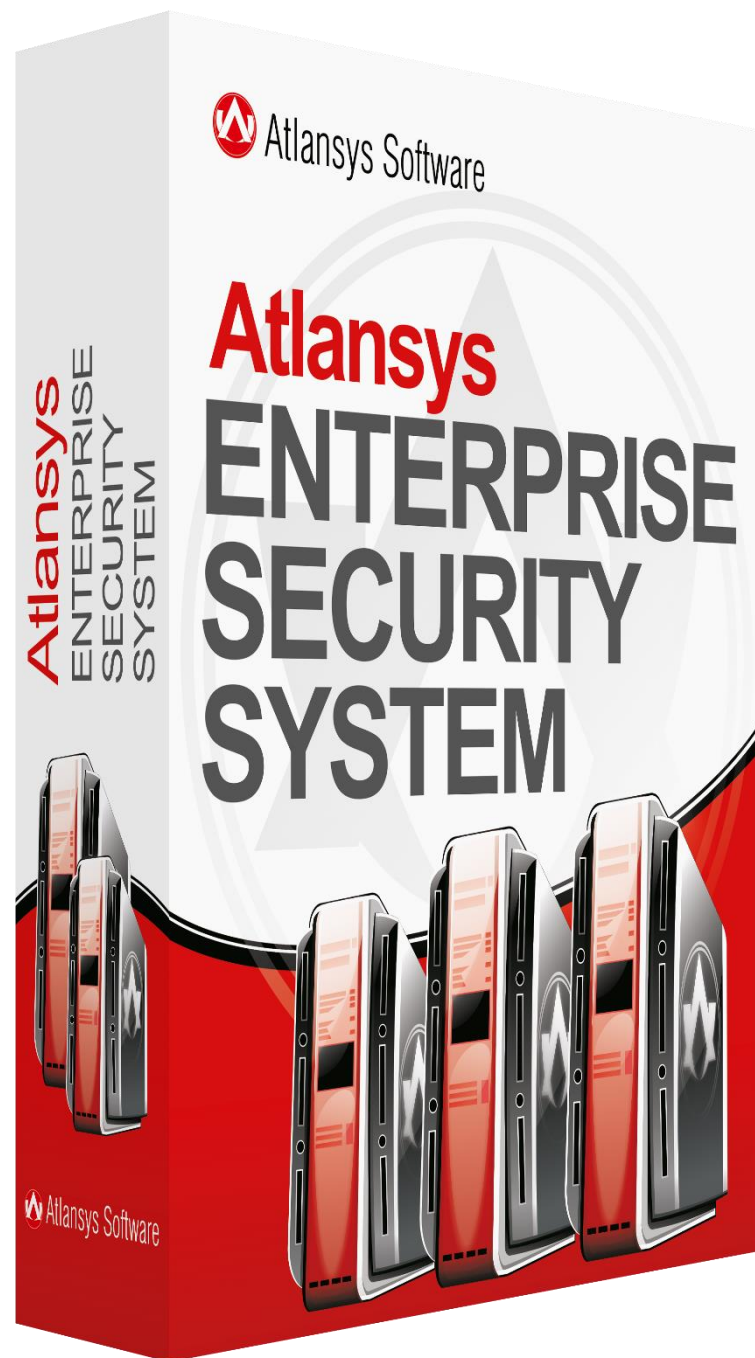
Atlansys ESS имеет положительное заключение ФСБ России о корректности встраивания в «Крипто ПРО CSP» и соответствует «Требованиям к шифровальным (криптографическим) средствам, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну» и «Требованиям к средствам электронной подписи» по классам КС1/КС2 в зависимости от используемого варианта исполнения СКЗИ.

Atlansys ESS получило высокие оценки на российских и международных выставках (т.к. СеBIT, InterSecurityForum, InterSecurityRussia, Softool в номинации «Продукт года 2016» и т.д.) и лаборатории PC Mag RE.



ЛИЦЕНЗИРОВАНИЕ ATLANSYS ENTERPRISE SECURITY SYSTEM

- Лицензии выдаются по количеству ЦУ, в рамках которых закупается любое количество серверов безопасности и клиентов для защиты рабочих станций
- Скидка действует:
 - ✓ При покупке лицензии на более длительный срок
 - ✓ При больших заказах
- Дополнительно:
 - ✓ Доработка системы по требованию заказчика
 - ✓ Обучение специалистов
 - ✓ Техническая поддержка 2-го уровня



ОСНОВНЫЕ ЗАКАЗЧИКИ ATLANSYS SOFTWARE



Защищено: 12 000 рабочих мест



Защищено: 4 000 рабочих мест



Защищено: 7 500 рабочих мест



Защищено: 2 000 рабочих мест



МИНИСТЕРСТВО
ЗДРАВООХРАНЕНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ



МИНИСТЕРСТВО ФИНАНСОВ
РОССИЙСКОЙ ФЕДЕРАЦИИ



Олимпийский
стадион
«ФИШТ»



vancouver 2010



> 3000 КОМПАНИЙ ИСПОЛЬЗУЮТ РЕШЕНИЯ АТЛАНСИС

БИЗНЕС КЕЙСЫ

ATLANSYS SOFTWARE



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

- ✓ Защита от НСД при хранении КТ на рабочих станциях, vir-ноутбуках – ФЗ №98 ст.10 п.2
- ✓ Безопасный обмен КТ 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



Башнефть - Защищено 1000 рабочих мест.

- ✓ Защита от НСД при хранении КТ на ноутбуках для должностных лиц – ФЗ №98 ст.10 п.2 (кражи)
- ✓ Безопасный обмен конфиденциальной информацией с партнерами/подрядчиками - ФЗ №98 ст.10 п.2
- ✓ Централизованное управление процедурами шифрования – ISO27001: A12.3.1
- ✓ Защита ключей пользователей от потери и кражи (использование смарт-карт с RFID меткой) – ISO27001: A12.3.2



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

БИЗНЕС КЕЙСЫ

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 защищено 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:

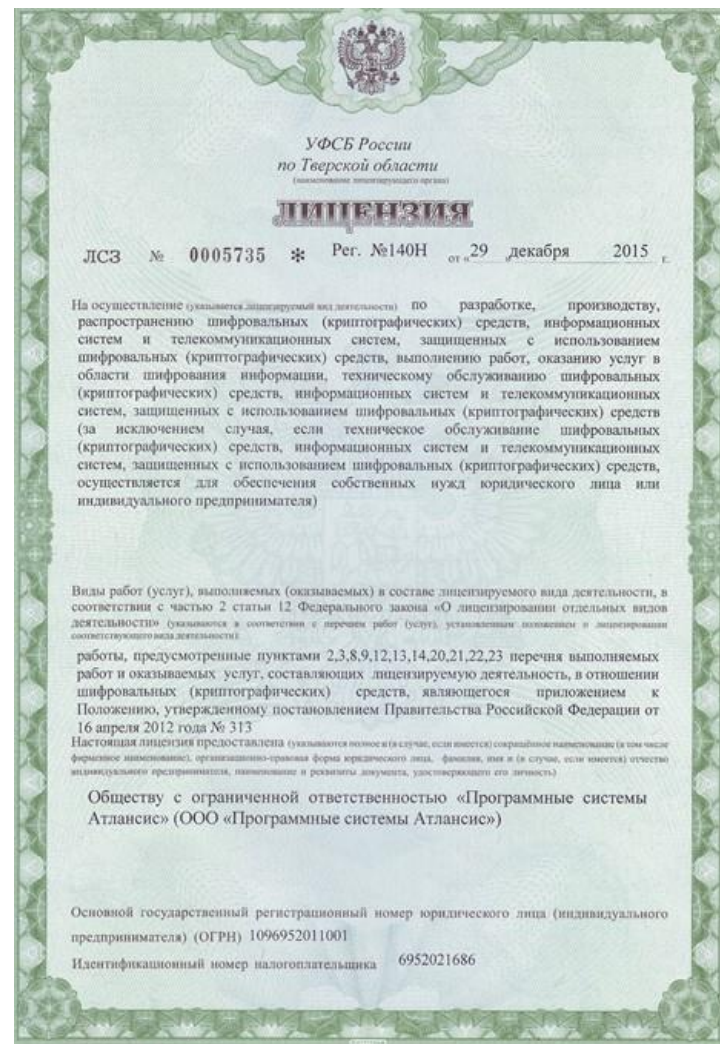
- ✓ На осуществление работ с использованием сведений составляющих государственную тайну №1324.
- ✓ На деятельность по разработке, производству, распространению шифровальных (криптографических) средств, информационных систем и телекоммуникационных систем, защищенных с использованием шифровальных (криптографических) 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.





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

Телефон: +7 (495) 470-09-92

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

Atlansys

ENTERPRISE SECURITY SYSTEM

