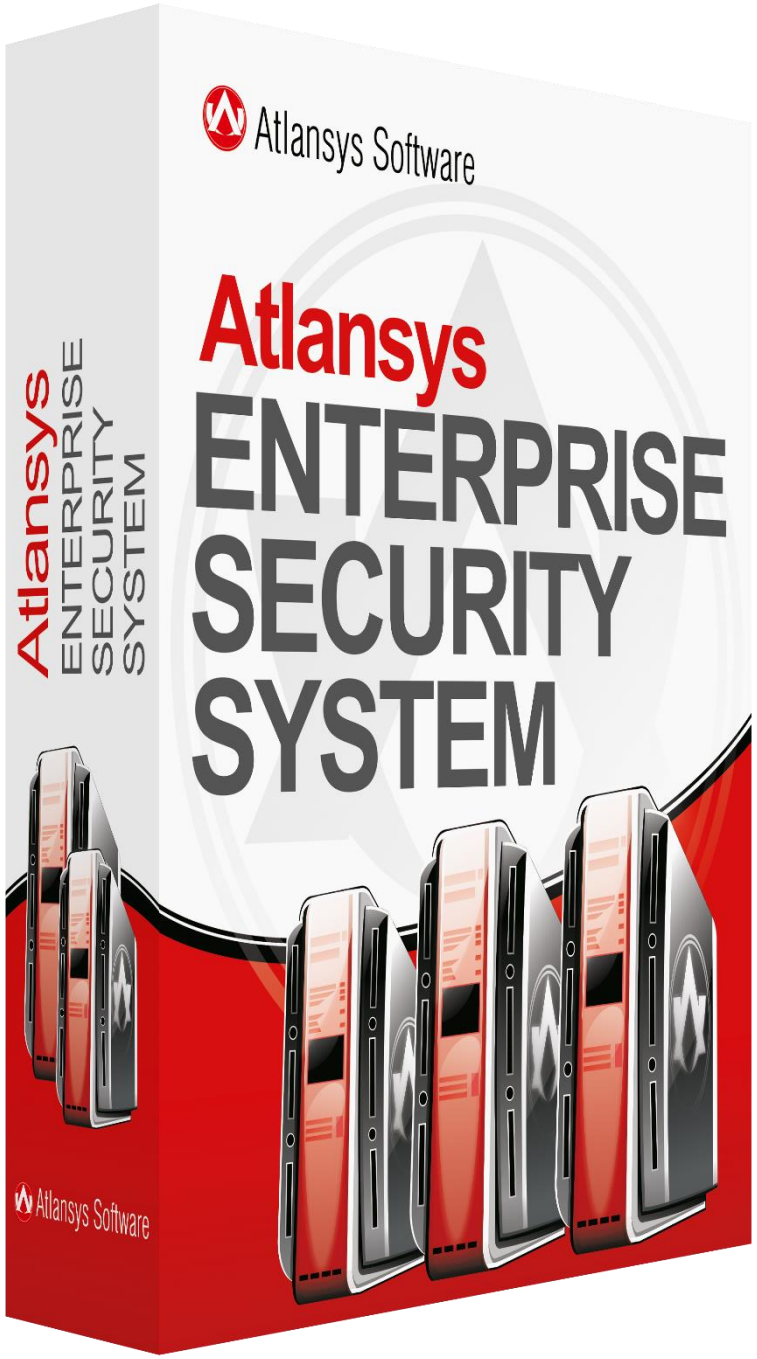
Atlansys Software

Atlansys
ENTERPRISE SECURITY SYSTEM

ATLANSYS ESS
НАЗНАЧЕНИЕ

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

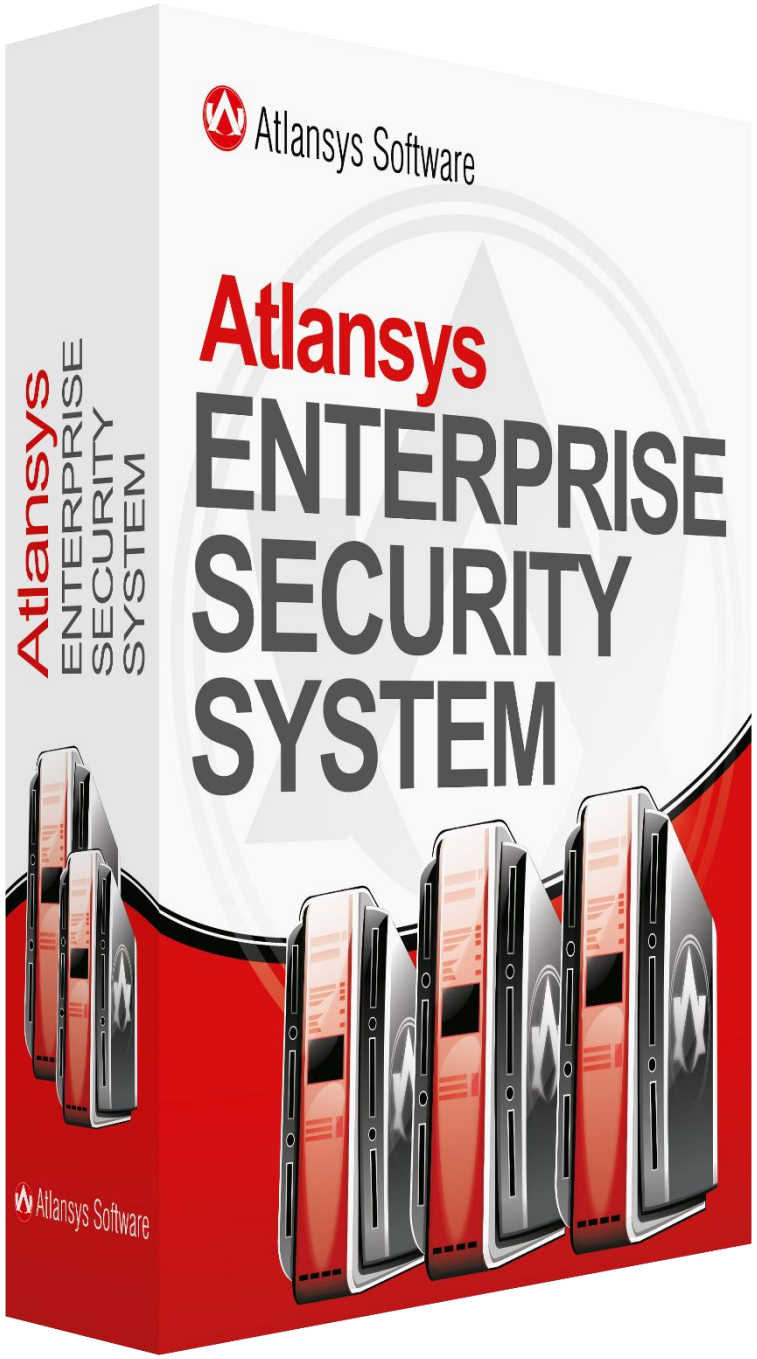
- ✓ ***Основное назначение – защита от НСД по средствам:***
  - ✓ *функций идентификации и аутентификации;*
  - ✓ *управления доступом;*
  - ✓ *шифрования документов при хранении и передачи;*
  - ✓ *контроля и защиты машинных носителей;*
  - ✓ *регистрации событий безопасности;*
  - ✓ *защиты данных обмена информационных систем за пределами контролируемой зоны.*
- ✓ ***На базе Atlansys ESS можно решать задачи*** *защиты критически важных объектов информационной инфраструктуры в рамках интеграции в СОИБ.*



ATLANSYS ESS ПРИМЕНЕНИЕ

Безопасность критически важных объектов информационной инфраструктуры достигается по средствам:

- ✓ *Защиты ИСПДн с уровнями УЗ2, УЗ3, УЗ4.*
- ✓ *Защиты документов при передаче по открытым каналам связи.*
- ✓ *Защиты от несанкционированного доступа к корпоративным ресурсам со стороны нарушителя.*
- ✓ *Шифрования ноутбуков (системный раздел, логические диски с базами данных).*
- ✓ *Создания/проверки электронной подписи документов по стандарту ГОСТ.*
- ✓ *Централизованного управления защищенными ресурсами и восстановления доступа к ним при утере сертификата или пароля пользователя.*
- ✓ *Защиты файловых и почтовых серверов, серверов приложений и файлов баз данных.*
- ✓ *Защиты локальных почтовых хранилищ на рабочих станциях и хранилища MS Exchange.*
- ✓ *Гарантированного уничтожения выбранных данных по средствам алгоритма ГОСТ.*



ATLANSYS ESS ТЕХНОЛОГИИ

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:

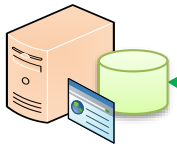
- ✓ *Поддержкой технологии электронной подписи документов (ЭП)*
- ✓ *По средствам обеспечению защиты хранимых на серверах ключей*

ATLANSYS ESS
АРХИТЕКТУРА РЕШЕНИЯ

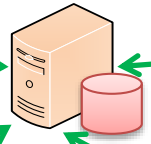
Atlansys ESS состоит из трех компонентов:

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

Защищенный Сервер



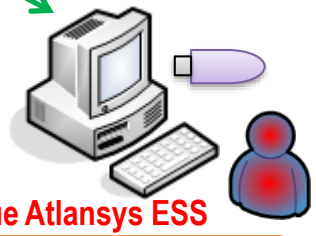
Сервер безопасности на базе Atlansys ESS



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)



Защищенные рабочие станции и ноутбуки

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

Удаленное управление Atlansys ESS

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

ATLANSYS ESS
СЕРВЕРНАЯ АРХИТЕКТУРА

Основные возможности ЦУ:

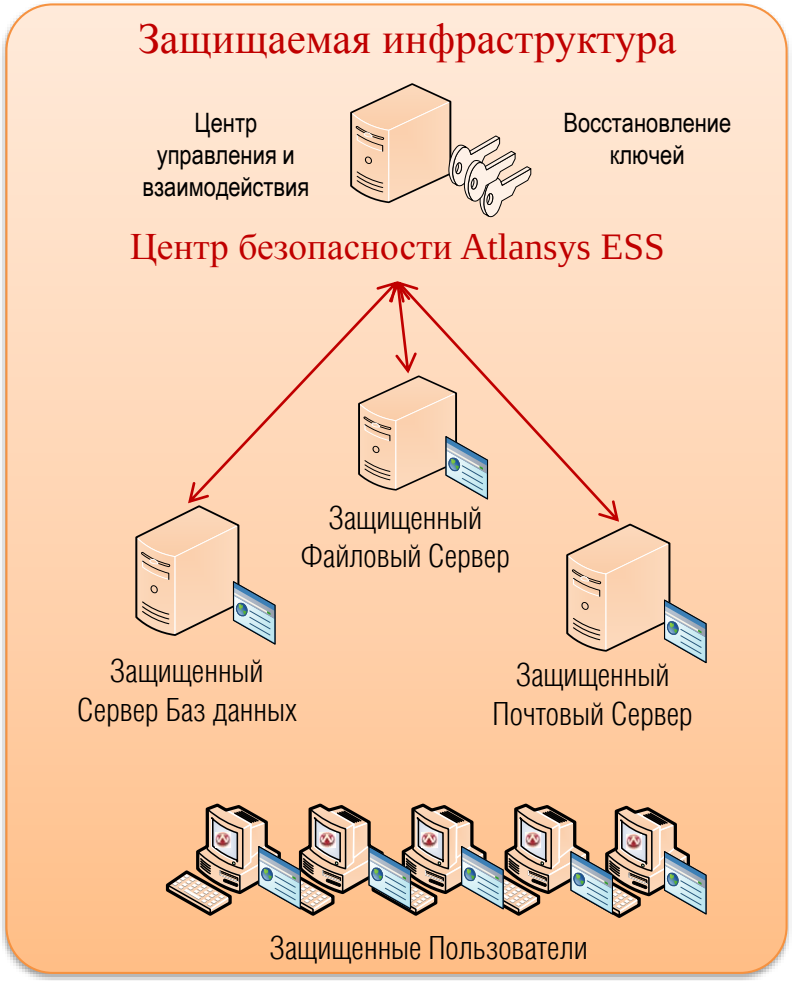
- ✓ *Интеграция с MS Active Directory и поддержка удостоверяющих центров организации*
- ✓ *Централизованное выполнение политик Красной кнопки «Тревоги»*
- ✓ *Централизованное развертывание системы на рабочие станции пользователей*
- ✓ *Высокая надежность системы (>10 тысяч пользователей на один Центр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



ATLANSYS ESS
ЗАЩИТА 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

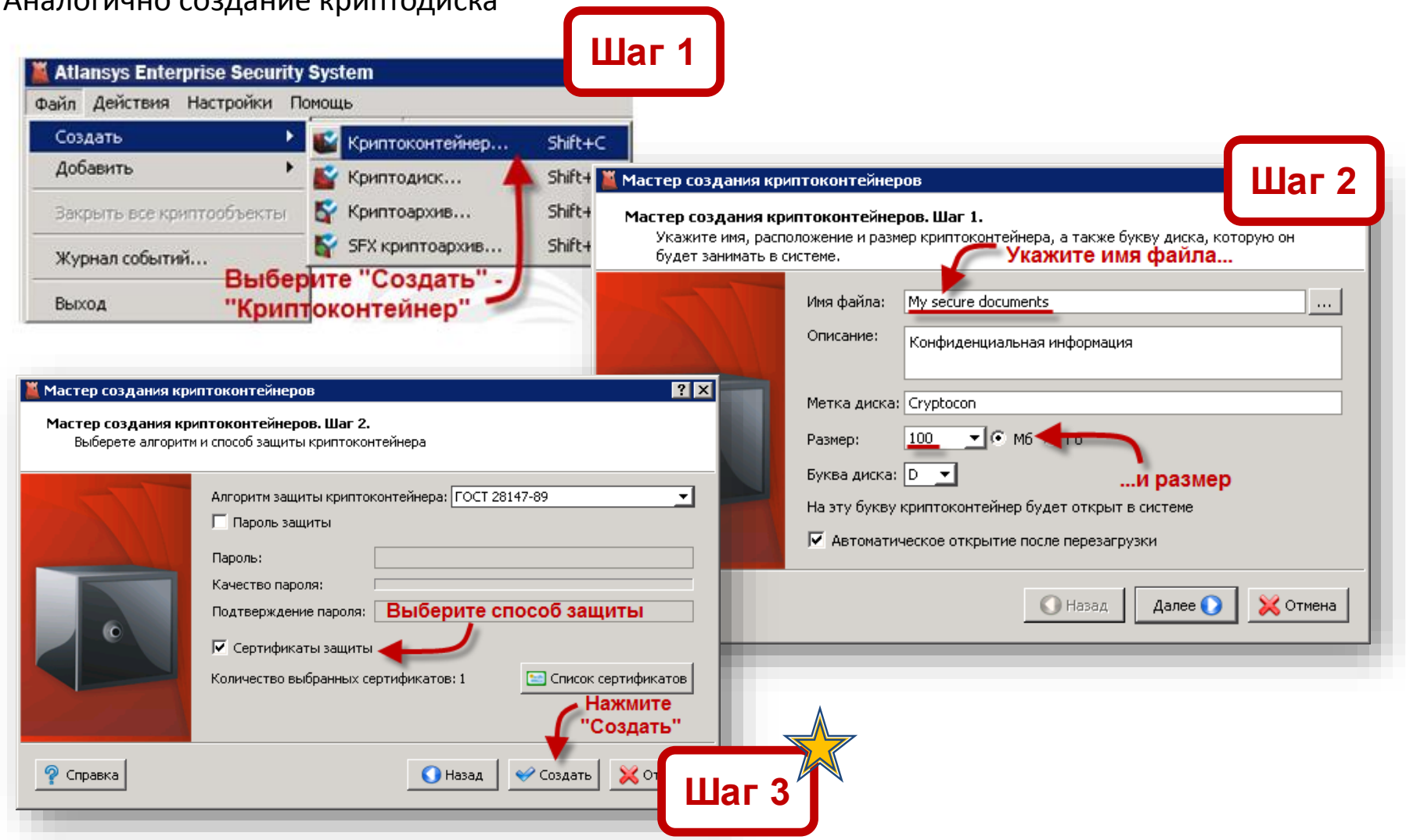
Автономный криптофлэш диск – это полностью зашифрованное съемное устройство (обычно это USB-flash накопитель), с которым можно работать, не имея установленного на компьютере клиента Atlansys ESS

Назначение: Хранение конфиденциальной информации на внешних носителях автономно

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

ATLANSYS ESS
СОЗДАНИЕ КРИПТОКОНТЕЙНЕРА

Аналогично создание криптодиска



УГРОЗЫ БЕЗОПАСНОСТИ ВНЕШНИХ НОСИТЕЛЕЙ В ОРГАНИЗАЦИИ

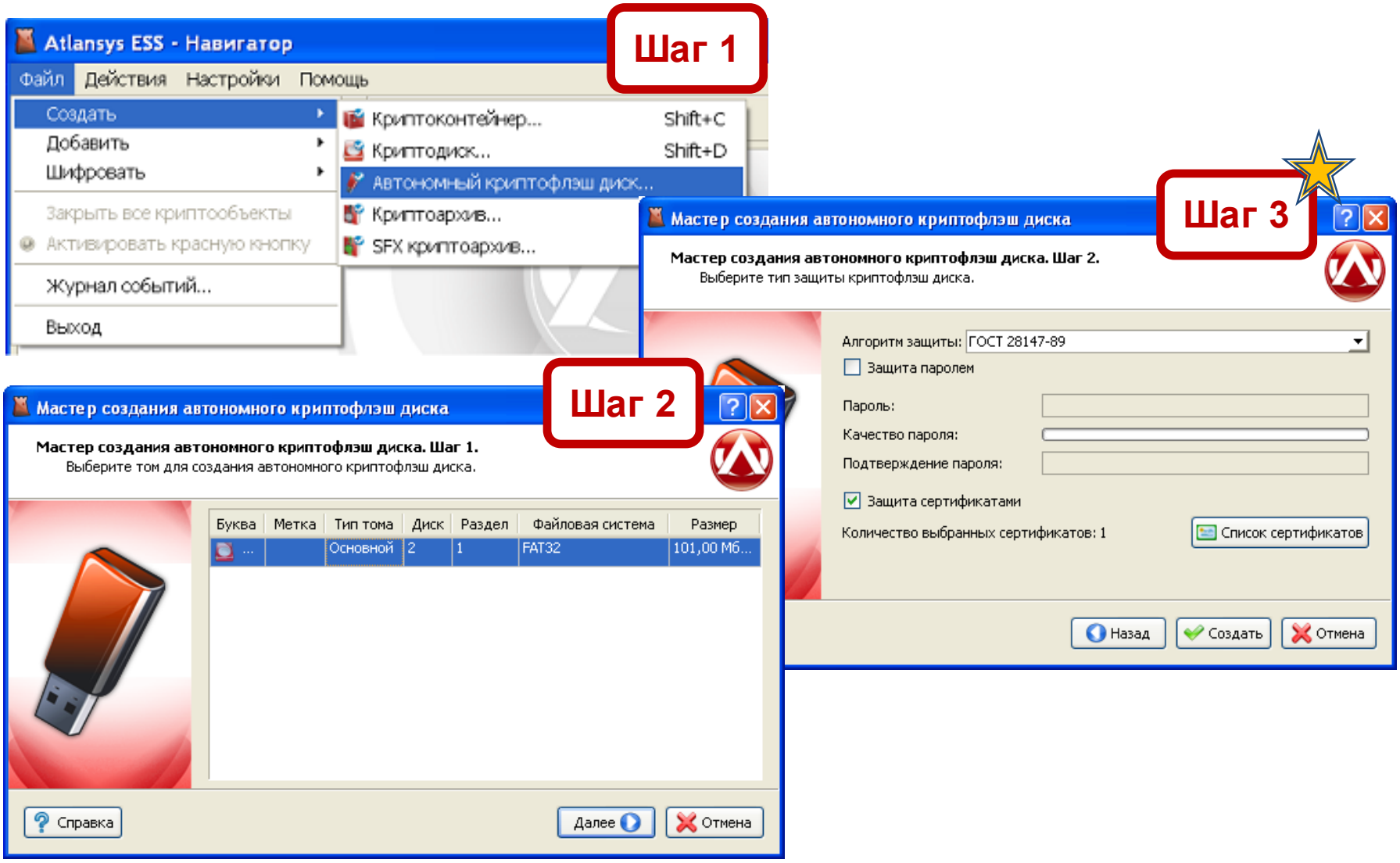
СЛЕДСТВИЕ УНИВЕРСАЛЬНОСТИ, МОБИЛЬНОСТИ И КОМПАКТНОСТИ:

- 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.)

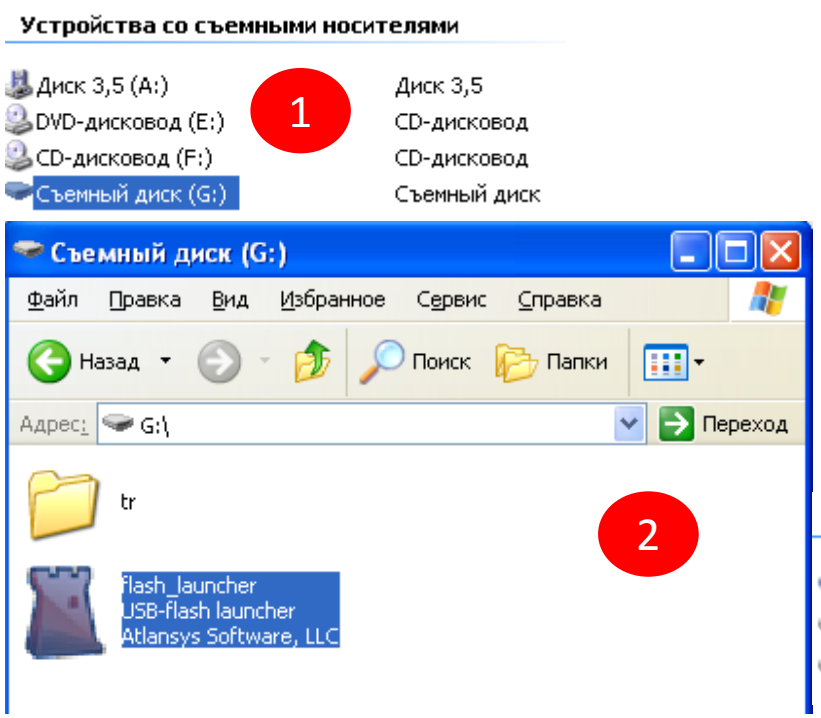
ATLANSYS ESS
СОЗДАНИЕ АВТОНОМНОГО КРИПТОФЛЭШ ДИСКА

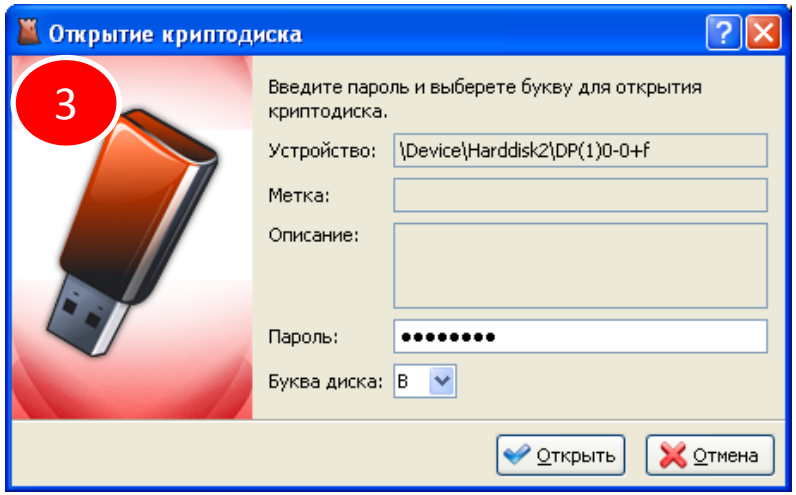


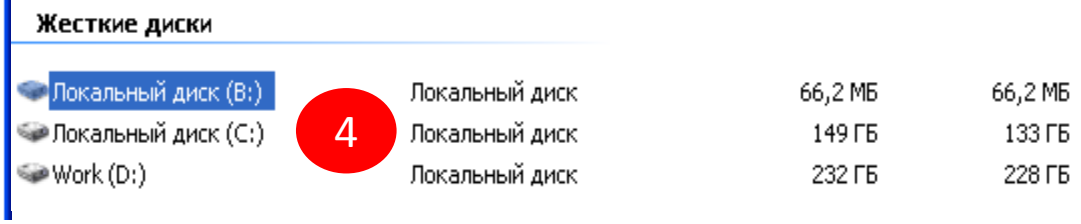
ATLANSYS ESS
РАБОТА С АВТОНОМНЫМ КРИПТОФЛЭШ ДИСКОМ

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.



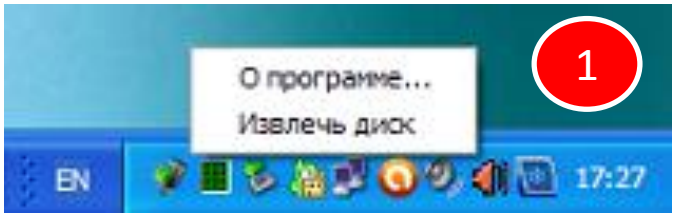




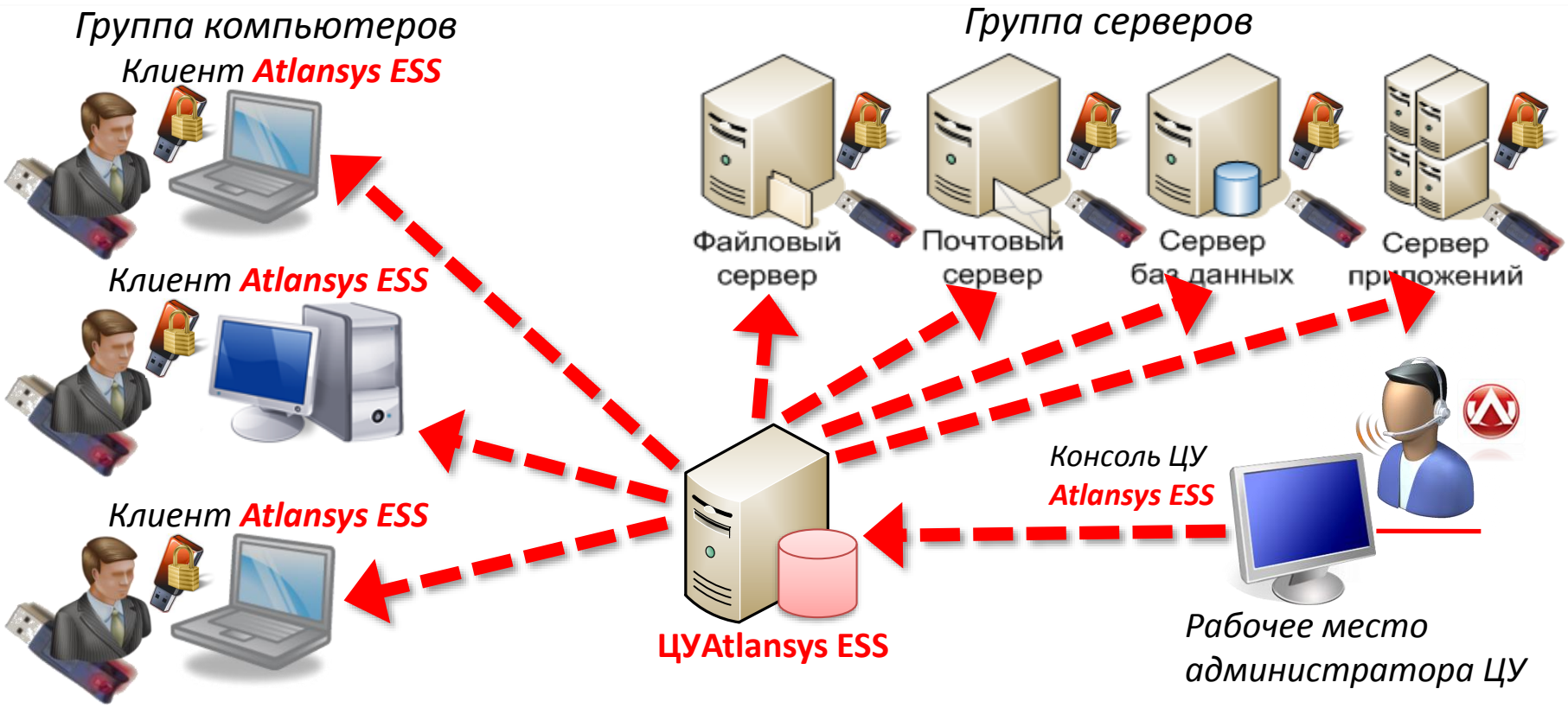
ATLANSYS ESS
РАБОТА С АВТОНОМНЫМ КРИПТОФЛЭШ ДИСКОМ

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.



ATLANSYS ESS
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

ATLANSYS ESS
ЗАЩИТА ИНФОРМАЦИИ ПРИ ПЕРЕДАЧЕ

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 по открытым каналам связи

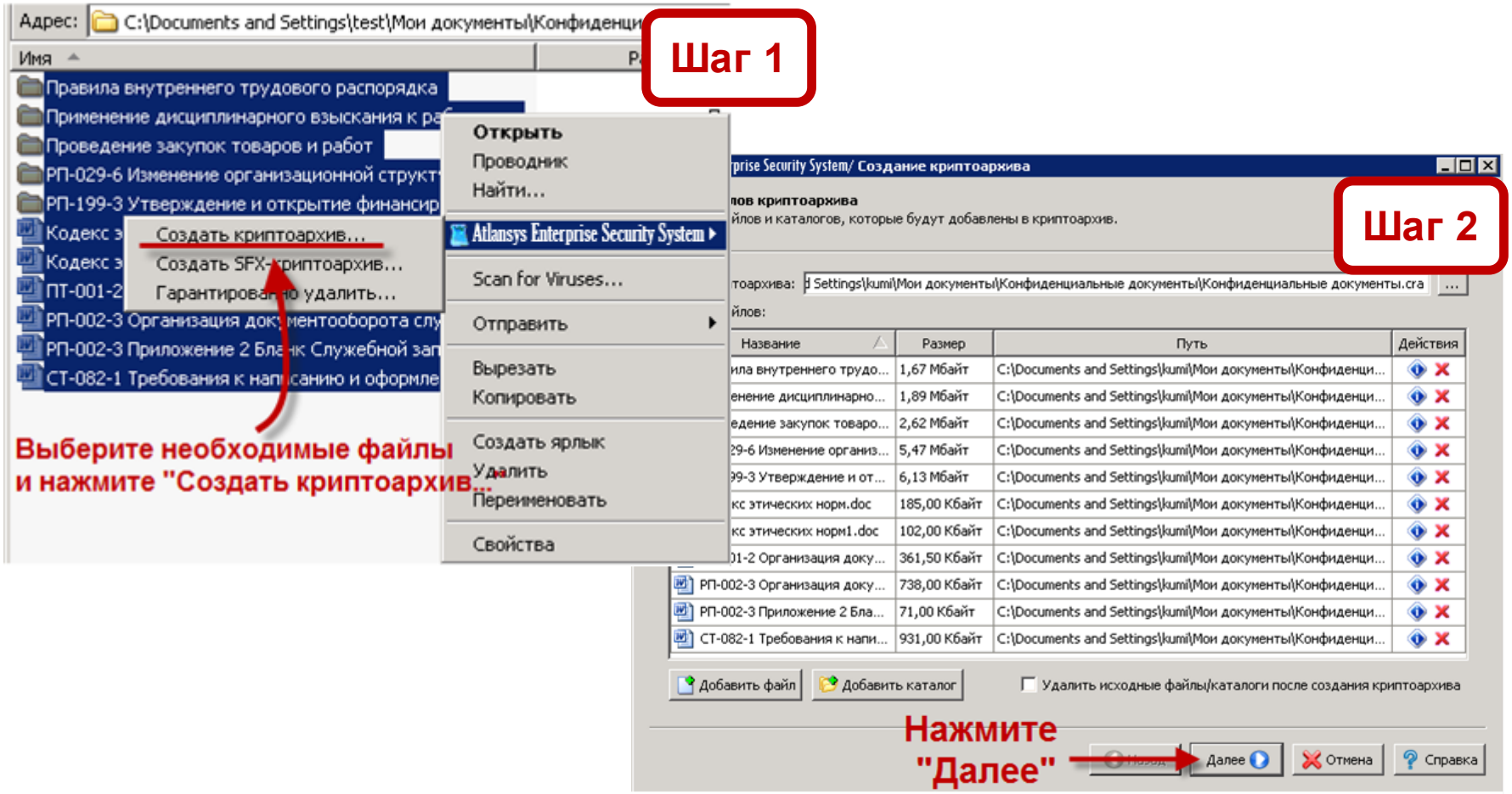
Автономный криптоархив – это сжатый зашифрованный файл, который открывается только по паролю без установки ПО Atlansys на компьютер пользователя

Назначение:

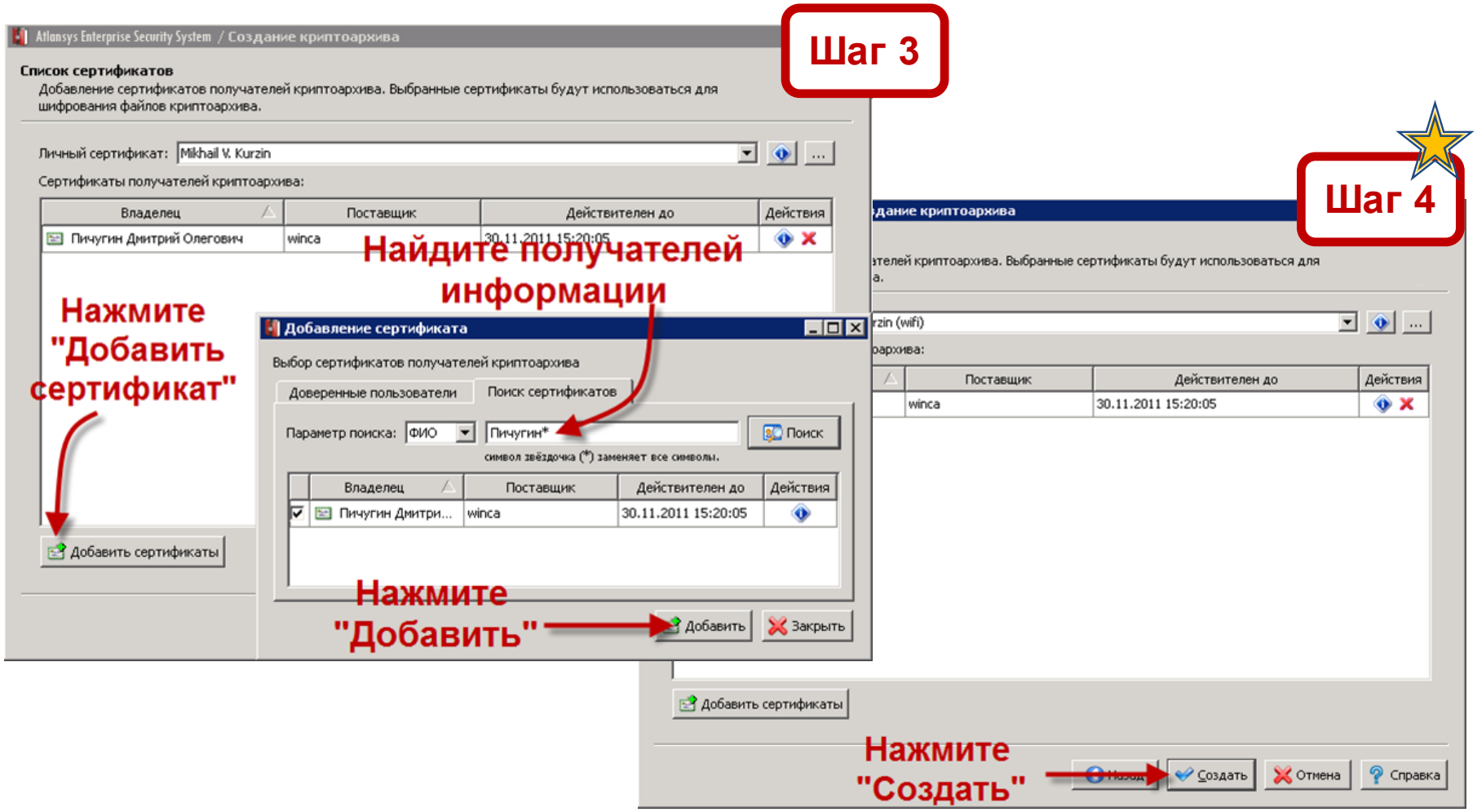
Обмен конфиденциальной информацией между сотрудниками и контрагентами в рамках NDA по открытым каналам связи

- 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.)

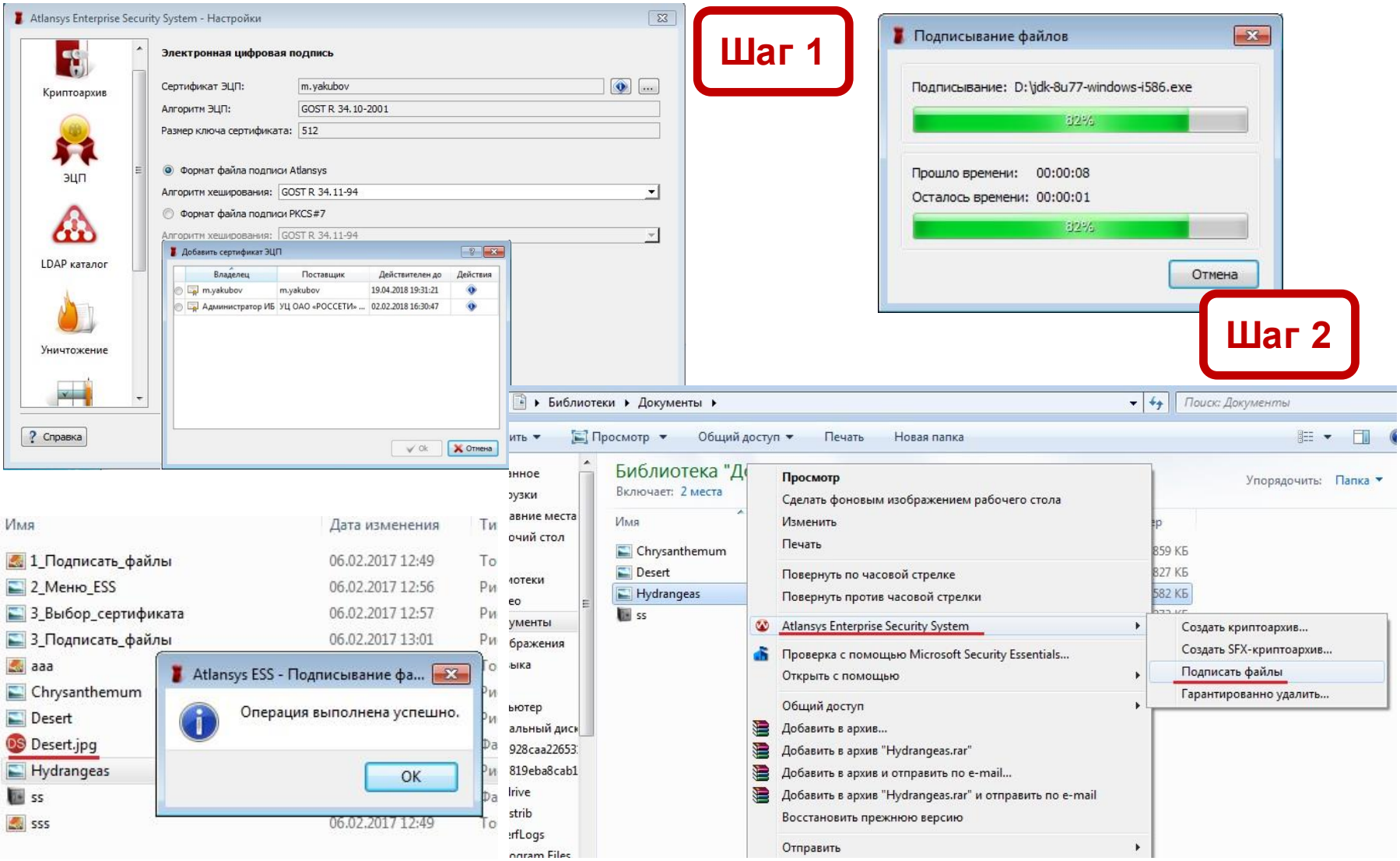
ATLANSYS ESS
СОЗДАНИЕ КРИПТОАРХИВА



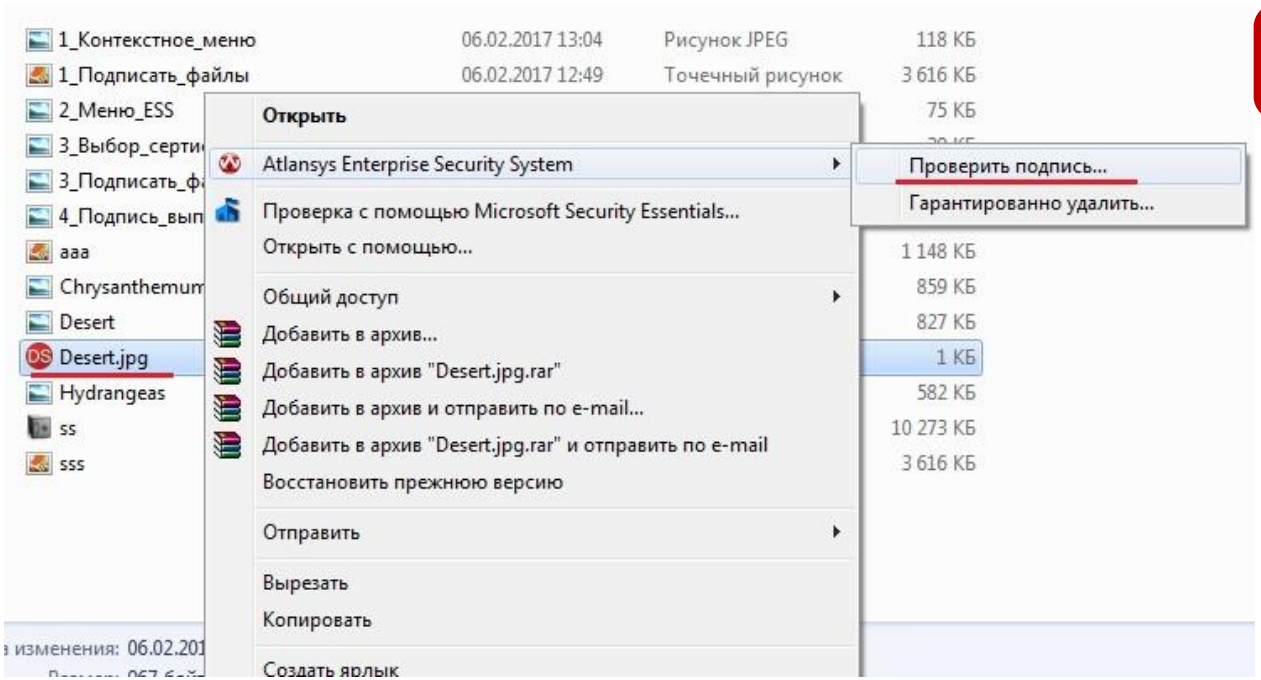
ATLANSYS ESS
СОЗДАНИЕ КРИПТОАРХИВА



ATLANSYS ESS
СОЗДАНИЕ ЭЛЕКТРОННОЙ ПОДПИСИ

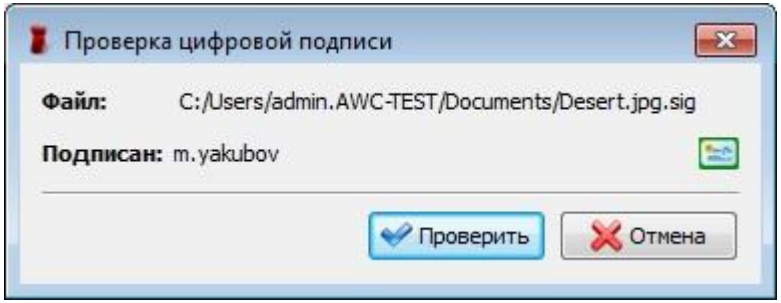


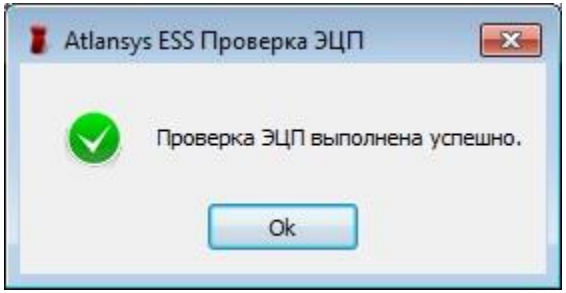
ATLANSYS ESS
ПРОВЕРКА ЭЛЕКТРОННОЙ ПОДПИСИ



Шаг 3

Шаг 4

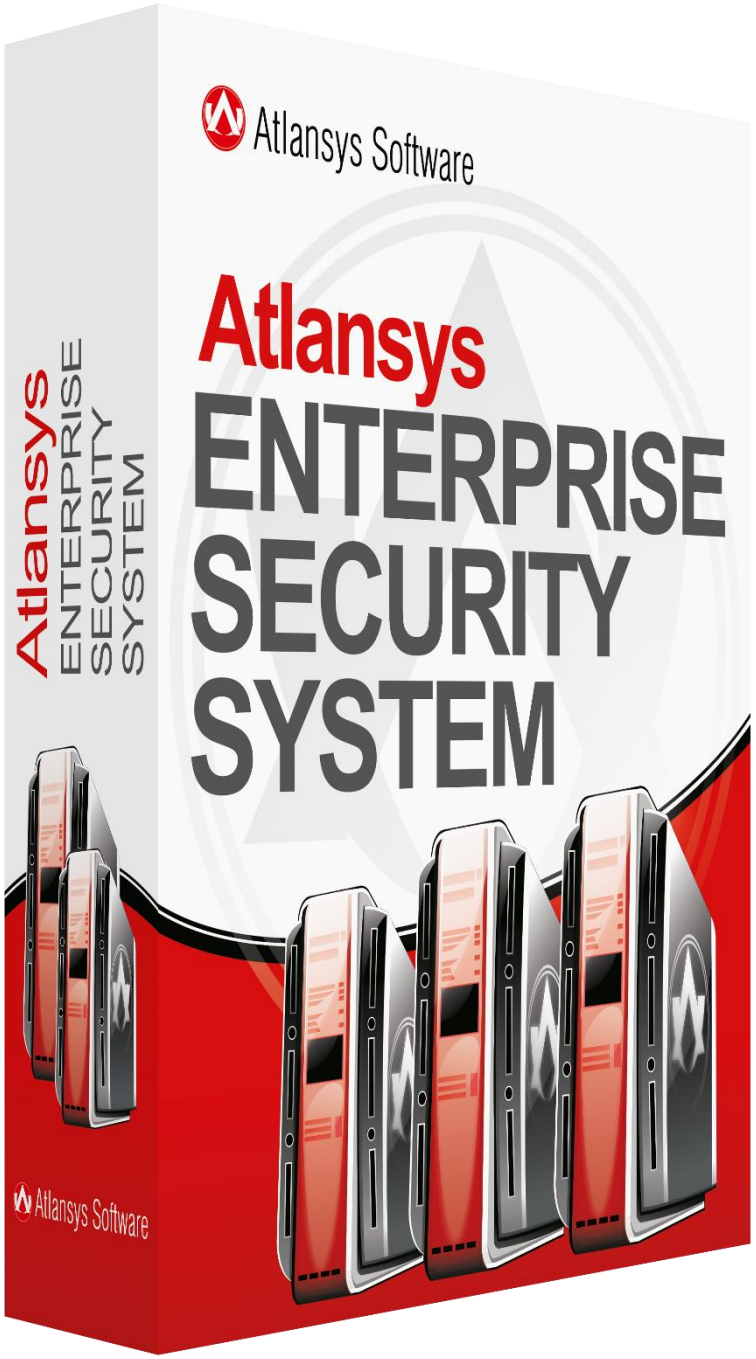




ATLANSYS ESS
ЗАДАЧИ

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 ESS ПРЕИМУЩЕСТВА

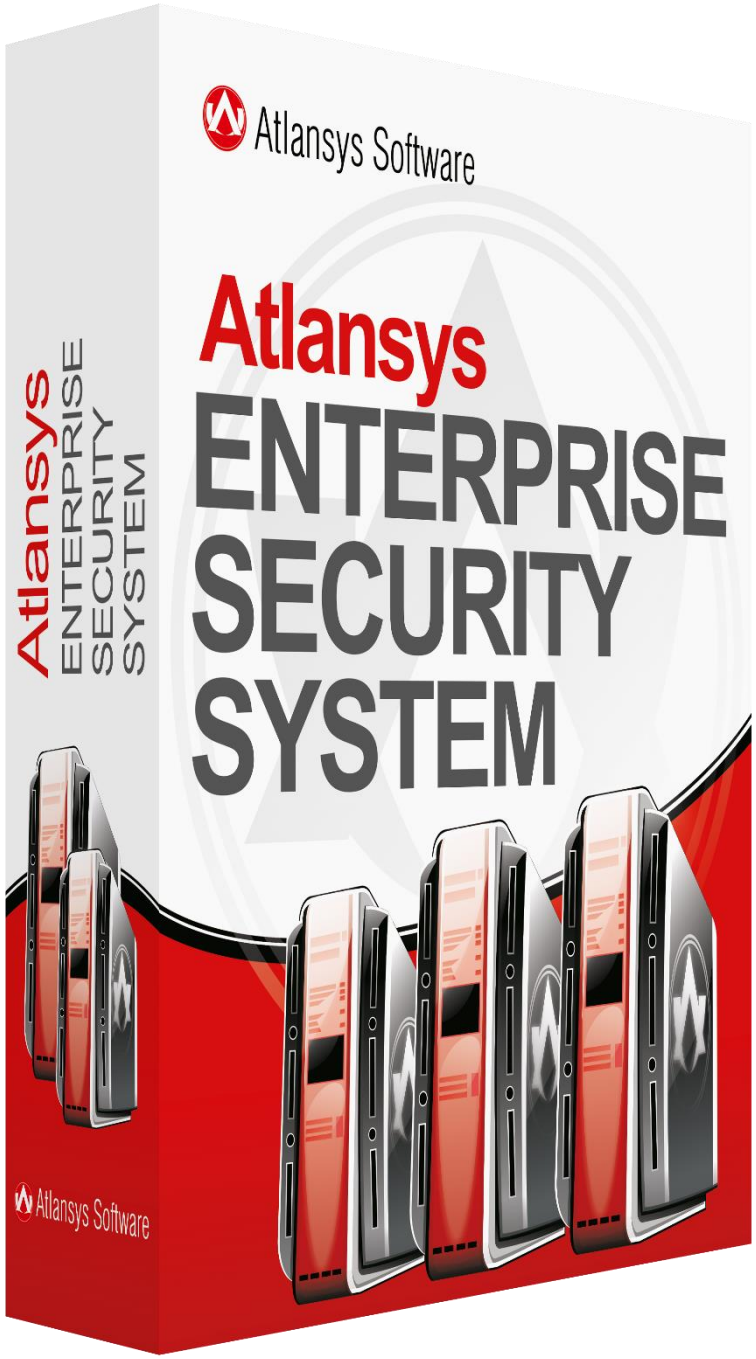
Решение Atlansys Enterprise Security System *зарегистрировано в едином реестре российских программ для ЭВМ и баз данных №2030 от 08 октября 2016 года Приказом Минкомсвязи России от 07.10.2016 №487.*

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… и к средствам электронной подписи» по классам КС1/КС2 в зависимости от используемого варианта исполнения СКЗИ.*

Atlansys ESS *выполняет требования регуляторов:*

- ✓ *ФЗ №187 «О безопасности критической информационной инфраструктуры РФ», ФЗ №152 «О персональных данных», ФЗ №98 «О коммерческой тайне», Приказ ФСТЭК №21, ГОСТ Р ИСО 27001-2006.*
- ✓ *Постановление Правительства РФ №1236 «Об установлении запрета на допуск иностранного программного обеспечения»*

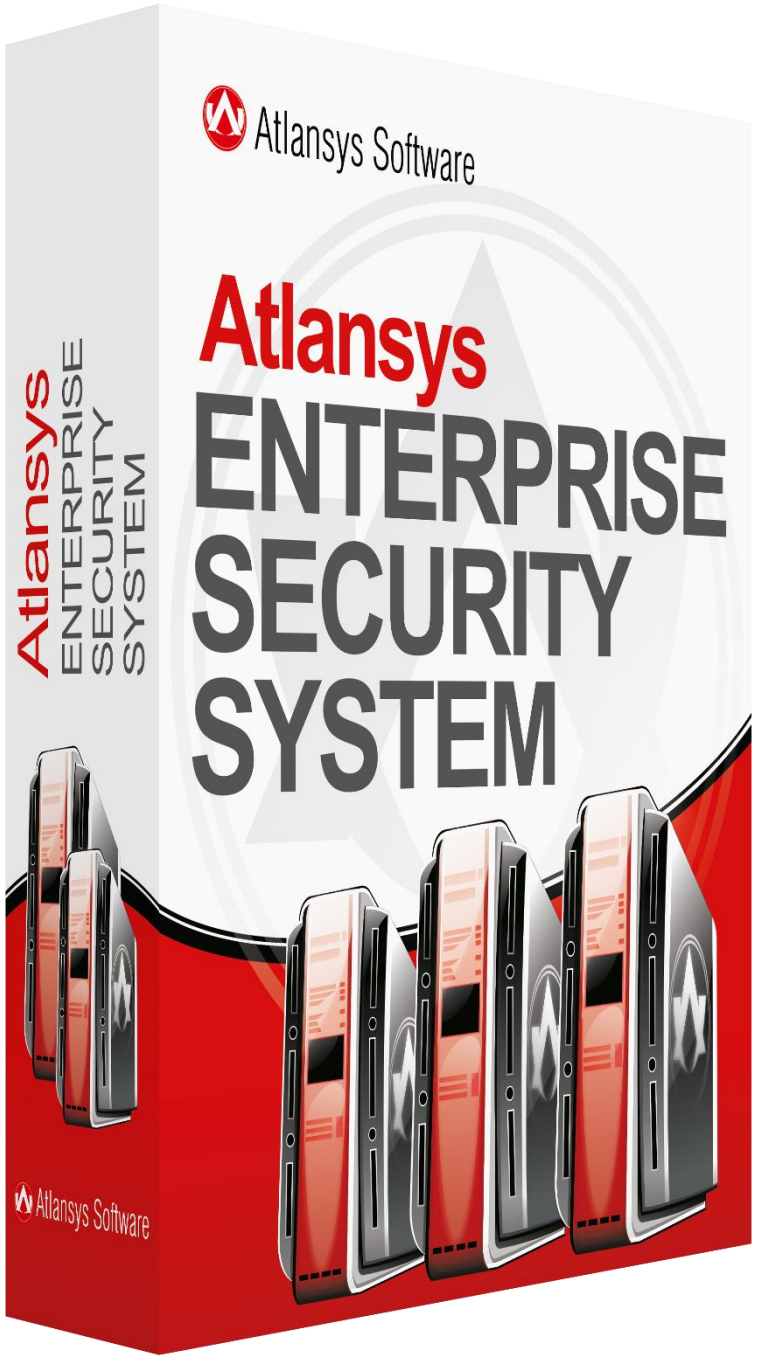
Atlansys ESS *получило высокие оценки на российских и международных выставках (CeBIT, InterSecurityForum, InterSecurityRussia, Softool в номинации «Приоритет 2019» и др.) и лаборатории PC Mag RE.*



ATLANSYS ESS ЛИЦЕНЗИРОВАНИЕ

ЛИЦЕНЗИРОВАНИЕ ПРОДУКТА

- Лицензии выдаются по количеству Центров Управлений, в рамках которых закупается любое количество серверов безопасности (Криптосерверов) и клиентов для защиты рабочих станций
- Скидка действует:
  - ✓ *При покупке лицензии на длительный срок (более 24 месяцев)*
  - ✓ *При больших заказах (более 2 тыс. ПК)*
- Дополнительно:
  - ✓ *Доработка системы по требованию заказчика (в рамках технической поддержки 2-го уровня)*
  - ✓ *Обучение специалистов*
  - ✓ *Техническая поддержка 1, 2-го уровня*



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

БИЗНЕС КЕЙСЫ
ATLANSYS SOFTWARE

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

- ✓ *Защита от НСД при хранении КТ на рабочих станциях, vip-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.*

МИНИСТЕРСТВО ФИНАНСОВ РОССИЙСКОЙ ФЕДЕРАЦИИ

Защищено 200 рабочих мест и 10 серверов.

- ✓ *Шифрование ноутбуков и рабочих станций сотрудников.*
- ✓ *Контроль и защита внешних носителей в компании.*
- ✓ *Защита файловых серверов и серверов баз данных.*

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)

Виды работ (услуг), выполняемых (оказываемых) в составе лицензируемого вида деятельности, в соответствии с частью 2 статьи 12 Федерального закона «О лицензировании отдельных видов деятельности

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

Настоящая лицензия предоставлена

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,
офис 300/13

Телефон: +7 (495) 470-09-92

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

Atlansys Software

Atlansys
ENTERPRISE SECURITY SYSTEM