



DEVICEPRO® ULTIMATE ОБЗОР ПРОДУКТОВ УПРАВЛЯТЬ УСТРОЙСТВАМИ ЛЕГКО И ПРОСТО!



devicepro
applicationpro
cryptionpro
cryptionpro HDD
Erasepro
Powerpro

Сертификат средств защиты информации по требованиям безопасности информации

Руководящий документ	Параметр	Значение
«Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (Гостехкомиссия России, 2002)	ОУД	2
«Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недеklarированных возможностей» (Гостехкомиссия России, 1999)	Отсутствие НДВ	4
	Класс защищенности	1Г
	Использование в ИСПД	K1 вкл.



Техническая информация

devicepro

- Управление устройствами
- Управление электропитанием
- Безвозвратное удаление данных

applicationpro

- Белый список в основе управления приложениями

DevicePro®
Ultimate

cryptionpro

- Шифрование данных на устройствах

cryptionpro HDD

- Шифрование жесткого диска

Архитектура  cynapro.

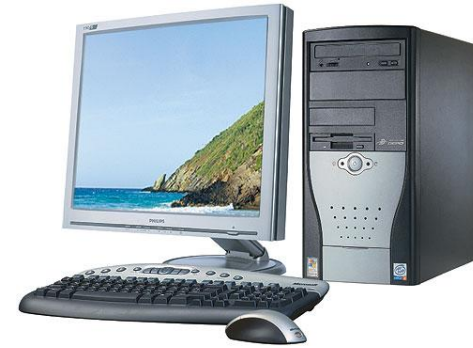


Требования к программному обеспечению

Сервер Cynapro



Клиенты Cynapro «Агенты»



SQL-Server:

- SQL-Server 2000 SP3a
- SQL-Server 2005
- SQL-Server 2005 Express Edition
- SQL-Server 2008
- SQL-Server 2008 Express Edition
- MSDE (Microsoft SQL-Server Database Engine)
- MySQL 5 или выше (ODBC обязательно)

Служба каталога:

- Active Directory
- Novell Client 4.91 SP2 oder höher
- OpenLDAP

- Windows 2000 (SP4 + RollUp 1)
- Windows XP + SP2/SP3 32/64 Bit
- Windows Vista (+ SP1) 32 und 64 Bit
- Windows 7 32 и 64 Bit

Минимальные требования к оборудованию

Сервер Cynapro



Pentium-IV, ОЗУ 1 Гбайт, HDD 120 Гбайт

Клиенты Cynapro
«Агенты»

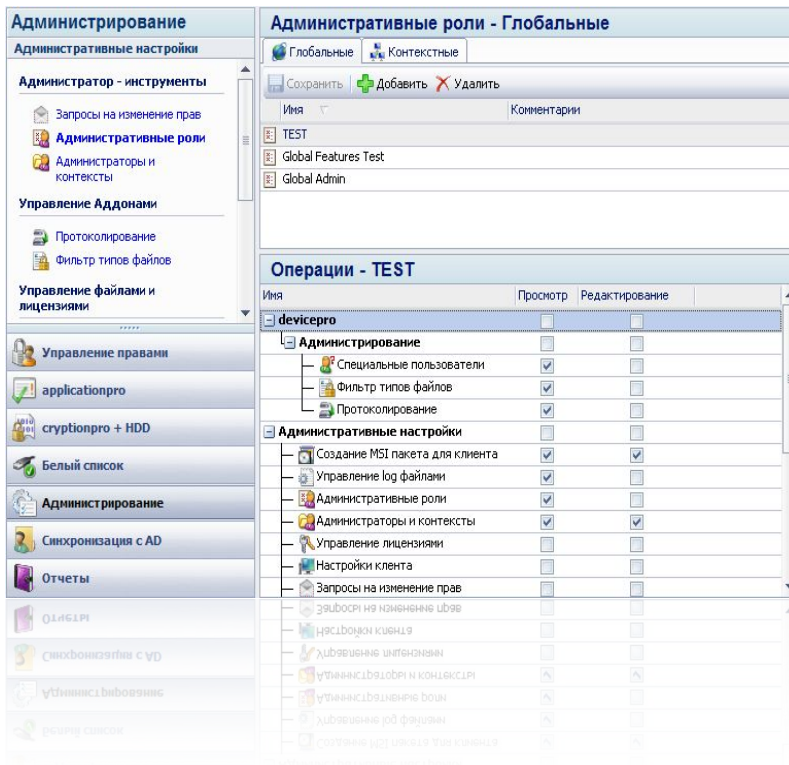


Pentium III с ОЗУ 128 Мбайт

Интуитивно понятный интерфейс

- Многоязычная консоль управления.

Доступ к административным областям может быть разрешен с использованием различных уровней прав, в зависимости от того, кто использует приложение (Supervisor, Administrator)



Интуитивно понятный интерфейс

devicepro

applicationpro

serverpro

serverpro HDD

- Автоматическая синхронизация с MS Active Directory / Novell eDirectory/ LDAP (Linux)
 - ✓ cynapro не вносит никаких изменений в Вашу структуру службы каталогов, вся информация копируется в базу данных и при необходимости обновляется
 - ✓ В отличии от других решений, cynapro не создает свои политики в AD, что позволяет так же управлять клиентами вне AD

- Возможность создавать собственную структуру.
- Автоматическое распределение и обновление (Push/Pull) агентов.
- Драйвер ядра минимизирует распределение ресурсов на клиенте.
- Использование сети и регулирование пропускной способности
 - ✓ Клиенты загружают и устанавливают обновления по предусмотренному графику, как это установлено

Настройки автоматического обновления

Одновременное скачивание:	<input type="text" value="20"/>	клиентов
Макс. загрузка сети:	<input type="text" value="30"/>	%
Параметры скачивания:		
<input type="radio"/> вручную <input type="radio"/> автоматически <input checked="" type="radio"/> по расписанию		
	<input type="text" value="8/ 7/2008"/>	<input type="text" value="14:15"/>
Параметры обновления:		
<input checked="" type="radio"/> сразу <input type="radio"/> по расписанию		
	<input type="text" value="8/ 7/2008"/>	<input type="text" value="14:15"/>
<input type="checkbox"/> Разрешить переименование		

Поддерживаемые устройства

deviserpro поддерживает следующие устройства:

- ✓ Дисководы
- ✓ CD/DVD
- ✓ Внешние накопители USB
- ✓ Несъёмные HDD
- ✓ Карты памяти SD/MMC
- ✓ Инфракрасный порт
- ✓ FireWire
- ✓ ТВ-тюнеры
- ✓ Bluetooth
- ✓ Смартфоны
- ✓ Blackberries
- ✓ Беспроводная сеть (WiFi)
- ✓ Параллельный порт
- ✓ Последовательный порт
- ✓ Карты расширения PCMCIA
- ✓ PCI Express Cards
- ✓ и другие



...

Управление доступом

- Нет доступа
- Чтение
- Полный доступ
- Временный доступ
- Для управления в автономном режиме используется код доступа
- Протоколирование
- Журнал
- Теневое копирование

нет доступа
 только чтение
 полный доступ
 по расписанию

Временный доступ...
 Генерация кода доступа...

Zugriffsrechte - Zeitsegmentschema

Device: CD / DVD
 Benutzer: Aleksa Trnadel

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Montag																								
Dienstag																								
Mittwoch																								
Donnerstag																								
Freitag																								
Samstag																								
Sonntag																								

kein Zugriff
 Lesezugriff
 Vollzugriff

OK Abbrechen

Freischaltungscode generieren

Geräteklasse: Challenge-Response

Parameter:

Benutzer: Daniel Döring

Device: Floppy Disk

Zugriff: Vollzugriff

Gültig: bis zum nächsten Login

Zeit: bis zum nächsten Login
 bis zur Netzwerk Anmeldeung
 Zeitraum

Whitelist ignorieren

Code: E720E-0C2B-5EA7-4FE2

E855C-3E34-9A92-D466
 E8377-9A42-F5E9-7E7F
 E6F38-F458-C00F-67B3
 E0C04-F6A7-F1D5-364F
 E720E-0C2B-5EA7-4FE2

Generieren Schließen

Права доступа - dpro(DPROTEST)

Страница: 1

Удалять дубликаты за период: 5 Минут

Тип устройства	Доступ	Дата	Имя файла	Размер	Дата измен...
CD / DVD	чтение	10.07.2008...	E:\autorun.inf	145	13.02.2006 ...
CD / DVD	чтение	10.07.2008...	E:\autorun.inf	145	13.02.2006 ...
CD / DVD	чтение	10.07.2008...	E:\autorun.inf	145	13.02.2006 ...
External Storage	чтение	10.07.2008...	S:\System\Apps\LPGDB.xml	88	09.05.2008 ...
External Storage	чтение	10.07.2008...	S:\System\Apps\LPDB.xml	1536	14.03.2008 ...

devicepro
 applicationpro
 cryptionpro
 cryptionpro HDD

Способы управления правами

Права пользователя



Права компьютера



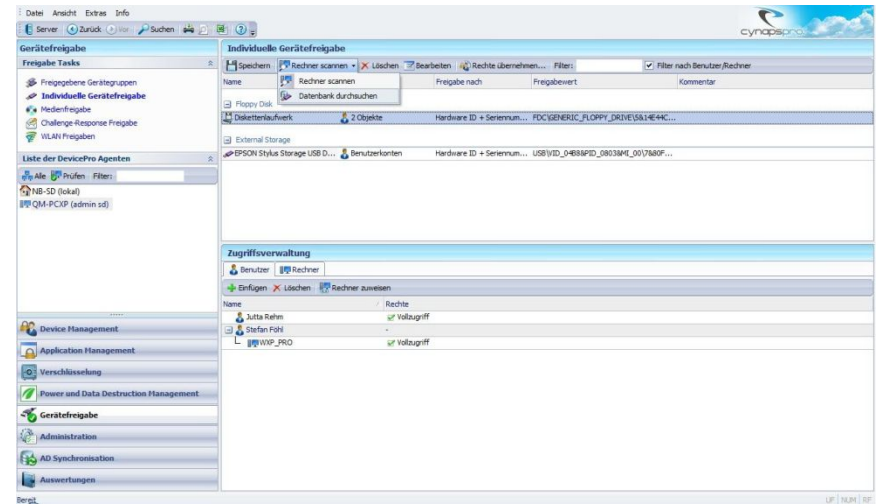
- Различают права пользователя, компьютера и комбинированные
 - ✓ Управление правами cynapro легко совмещается с основными принципами любой компании
 - ✓ Высший приоритет имеют права компьютера, следующие по значимости – права связки, наименьший – права пользователя

Черный и белый список оборудования

- Модели устройств и носителей:
 - Название
 - Hardware ID

Уникальные модели устройств

- Название
- Серийный номер
- Hardware ID
- Volume ID

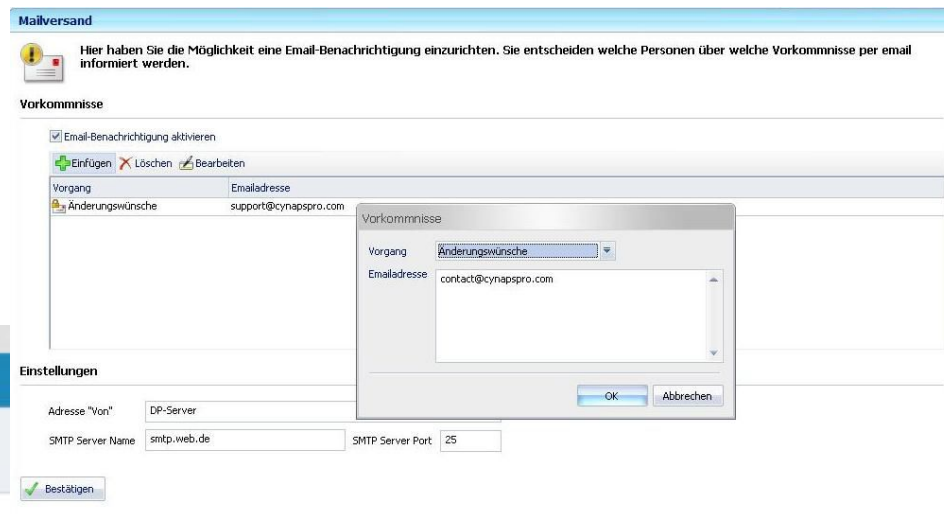
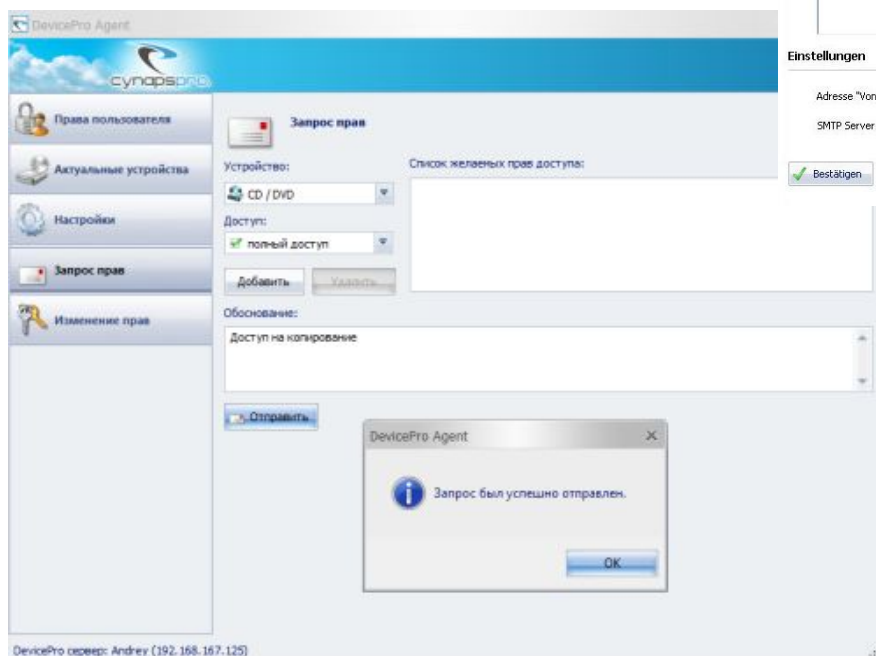


- Разрешенные беспроводные сети WLAN

Привязка носителей к пользователю или компьютеру

Уведомление электронной почтой

- Запросы на изменение прав доступа дублируются электронной почтой



Консоль для предоставления отчетности

devicepro

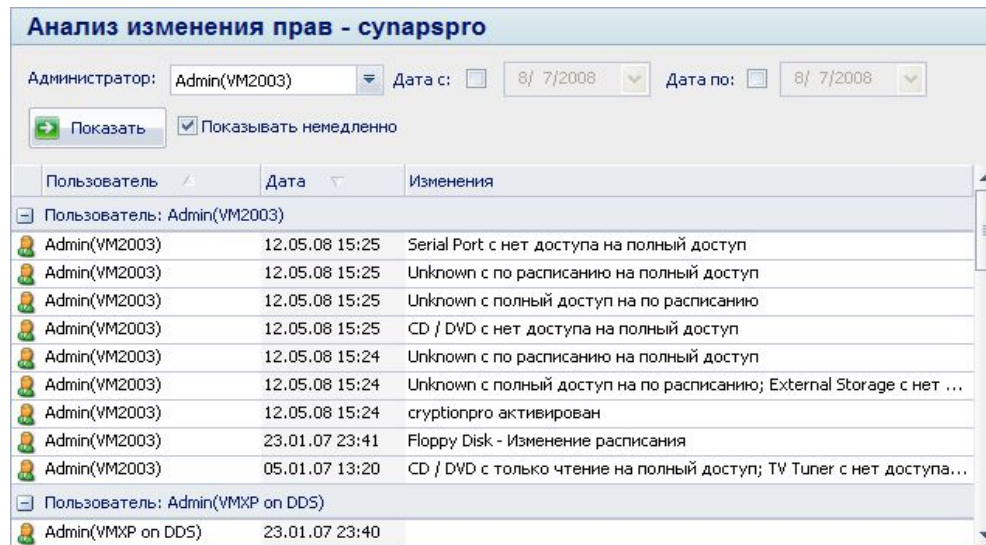
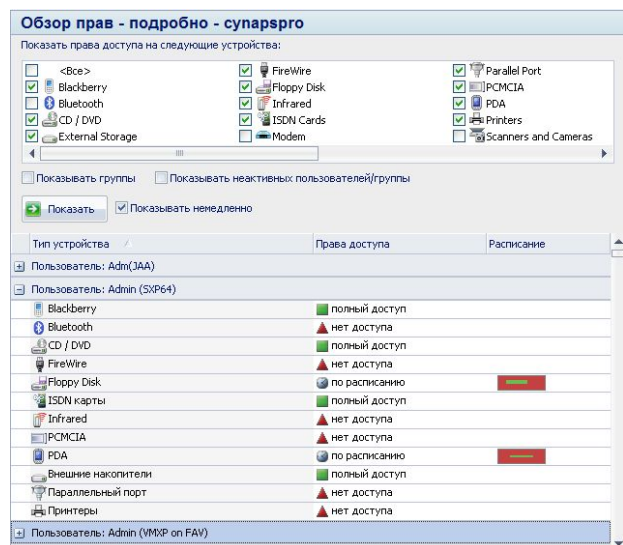
applicationpro

cryptopro

cryptopro HDD

- Детальный обзор прав

- ✓ Все права доступа можно просматривать в любое время
- ✓ Любые изменения прав прослеживаются, выводится информация о том когда, кто и почему произвел изменения
- ✓ Предусмотрен просмотр изменений за определенный период



Консоль для предоставления отчетности

- Статистика доступа и актуальность прав
 - ✓ Выводится вся информация об операциях пользователей по устройствам, в отдельных случаях – с именами файлов
 - ✓ „Пропавшие“ файлы могут быть найдены:
 - Пользователь, который имеет доступ к запросу на изменение прав
 - По устройству, на которое происходило копирование
 - По времени, когда было последнее изменение

Статистика обращений - cynapspro

Дата: с 7/31/2008 по 8/ 7/2008 Устройство: External Storage Операция: <Все>

Показывать немедленно

Устройство	Пользователь	Время	Доступ
06.08.2008			
External Storage	User (VMXP on FAV)	21:30:56	чтение
External Storage	User (VMXP on FAV)	21:12:48	запись
05.08.2008			
External Storage	User(VMXP on DDS)	17:03:17	чтение/запись
External Storage	User(VMXP on DDS)	17:02:21	чтение
External Storage	User(VMXP on DDS)	16:32:51	запись
04.08.2008			
31.07.2008			

Неактуальные права - pivm

Показывать неактивных пользователей

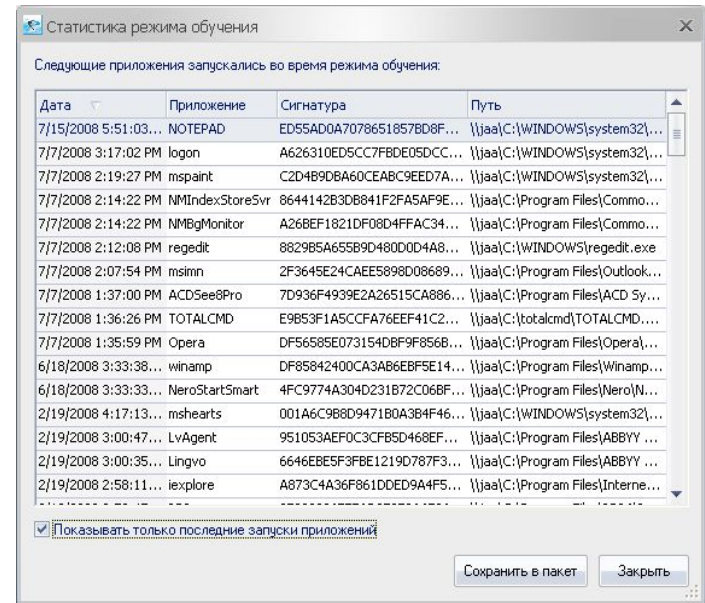
Показывать немедленно

Пользователь	Дата	Изменения
Пользователь: User_01_01_02		
User_01_01_02	07.07.08 14:05	Unklown с по расписанию на нет доступа...
User_01_01_02	22.04.08 13:16	devicepro активирован
Пользователь: User_01_02_01		
User_01_02_01	07.07.08 14:05	Unklown с по расписанию на нет доступа...
User_01_02_01	22.04.08 13:16	devicepro активирован
Пользователь: User_01_02_02		
User_01_02_02	07.07.08 14:05	Unklown с по расписанию на нет доступа...
User_01_02_02	22.04.08 13:16	devicepro активирован

Возможности applicationpro

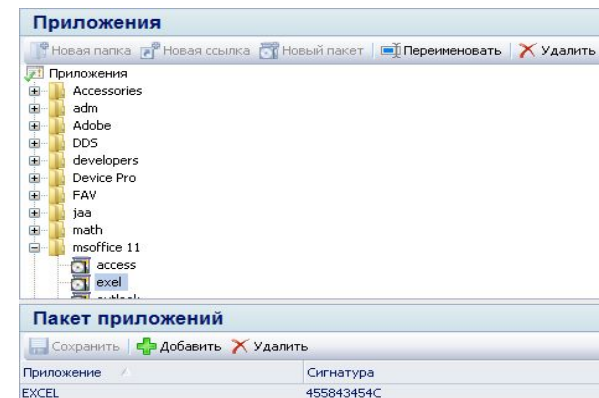
• Режим обучения

- ✓ Простое включение встроенного режима обучения, в результате которого показываются все запускаемые приложения
- ✓ Из списка выбираются приложения, с которыми будет разрешено работать пользователям, и добавляются в пакеты приложений



• Описание ролей и пакетов

- ✓ Пакеты приложений создаются в соответствии с их названием и предназначением, для удобства идентификации
- ✓ Роли объединяют в себе определенный набор пакетов или папок



Возможности и достоинства cryptionpro

- cryptionpro поддерживает различные способы шифрования
 - ✓ Автоматическое шифрование
 - ✓ Индивидуальное шифрование
 - ✓ Тип шифрования: AES 256 Bit
 - ✓ Тип шифрования: Blowfish 256 Bit
 - ✓ Шифрование вне сети, посредством мобильного
 - ✓ Master Password Management
 - ✓ Central Password Management
 - ✓ Права доступа базируются на группах или индивидуальных пользователях
 - ✓ Индивидуальные пользовательские сообщения

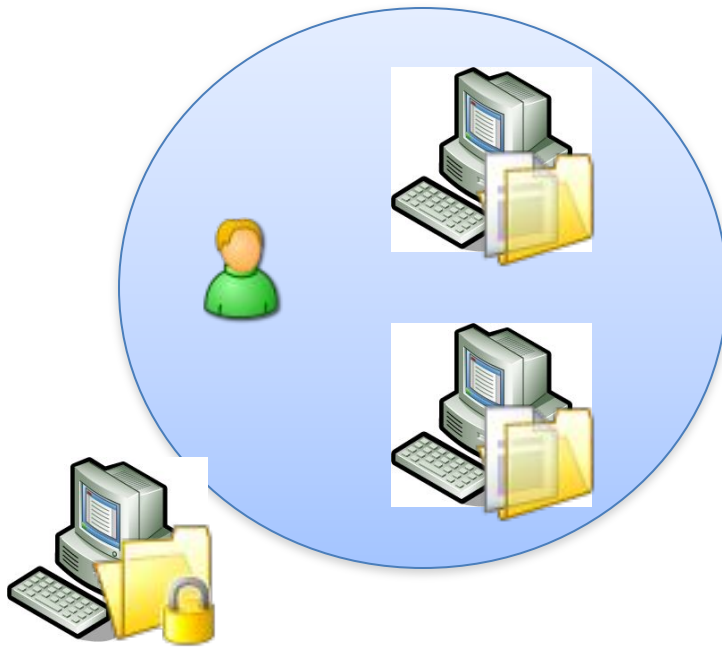
cryptionpro – как это работает

devicepro

applicationpro

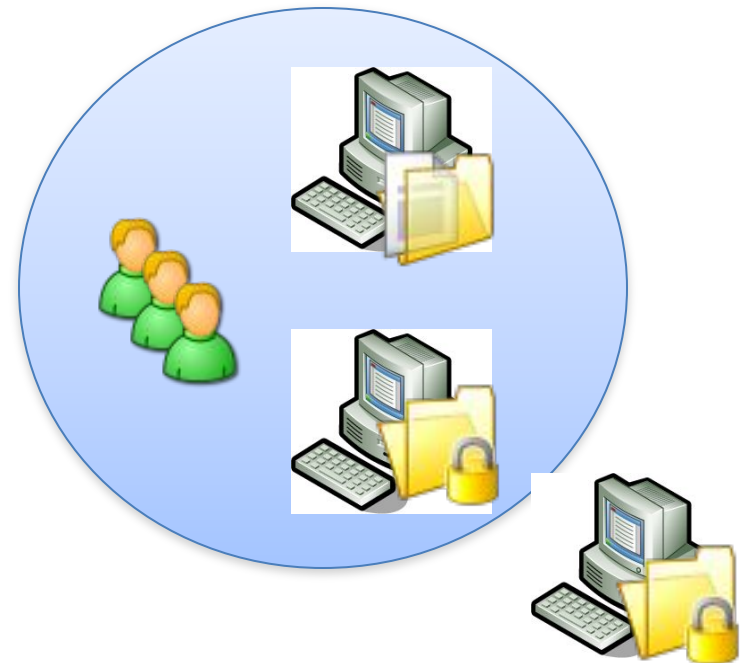
cryptionpro

cryptionpro HDD



Общее шифрование

- Файлы доступны только внутри сети
- Пользователь может (если разрешено) выбирать, какие файлы шифровать



Индивидуальное шифрование

- Пользователь может выбирать какие файлы шифровать и какой тип шифрования выбирать
- Только отдельные пользователи смогут открыть такие файлы внутри сети

Возможности и достоинства cryptionpro HDD

- cryptionpro HDD основано на Full Disk Encryption (FDE)
 - ✓ Драйвер шифрования в NTLoader и Microsoft Windows
 - ✓ Прозрачное шифрование надежными алгоритмами
 - AES, Triple-DES, Blowfish
 - ✓ Ключ шифрования может быть выбран или установлен по умолчанию
 - ✓ Выделение разделов основано на ключах шифрования
 - ✓ Шифрование секторов базировано на основании разделов
 - ✓ Шифрование операционной системы, файлов данных, временных файлов и hibernation (режим пониженного энергопотребления) файлов
 - ✓ Механизмы по восстановлению после непредвиденных ситуаций базируются на Bart-PE
 - ✓ Шифрование внешних устройств(USB и PCMCIA)

Возможности и достоинства cryptionpro HDD

- Пред загрузочная идентификация системы cryptionpro HDD
 - ✓ Запуск компьютера с жесткого диска системы Linux
 - ✓ Интегрированный механизм идентификации
 - Прозрачный метод (без идентификации)
 - Метод доступа Smartcard / PKCS#11
 - Основанный на данных учетной записи Windows (Имя пользователя, домен, пароль)
 - ✓ Интегрированное устройство управления запуском
 - ✓ Однократное введение пароля Microsoft Windows, Novell
 - Имя пользователя, домен, пароль
 - Сертификат X.509
 - ✓ Интегрированная служба поддержки при регистрации
 - Offline challenge / response with user helpdesk
 - Разблокировать Smartcard
 - Регистрация без Smartcard



Методы аутентификации cryptopro HDD

- Прозрачный режим

- ✓ Взаимодействие с пользователем не требуется
- ✓ Ключ замаскирован на диске
- ✓ Лэптоп загружает заставку Windows при идентификации
- ✓ Минимальный уровень защиты



Minimal

Security
Level

Методы аутентификации cryptonpro HDD

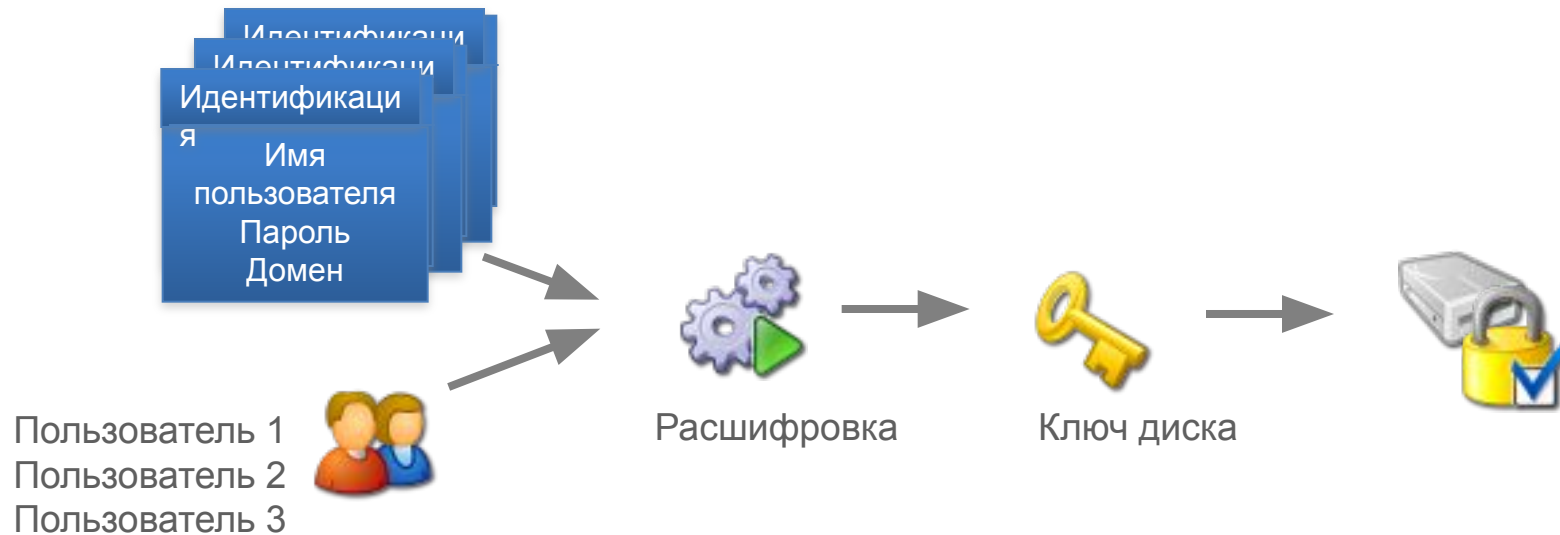
devicepro

applicationpro

cryptonpro

cryptonpro HDD

- Метод, основанный на данных учетной записи Windows
 - ✓ Предзагрузочная идентификация с ядром Linux
 - ✓ Ключ зашифрован с паролем пользователя
 - ✓ Однократное введение пароля Microsoft Windows, Novell
 - ✓ Многопользовательская поддержка
 - ✓ Средняя степень защиты



Medium

Security Level

Методы аутентификации cynapro HDD

devicepro

applicationpro

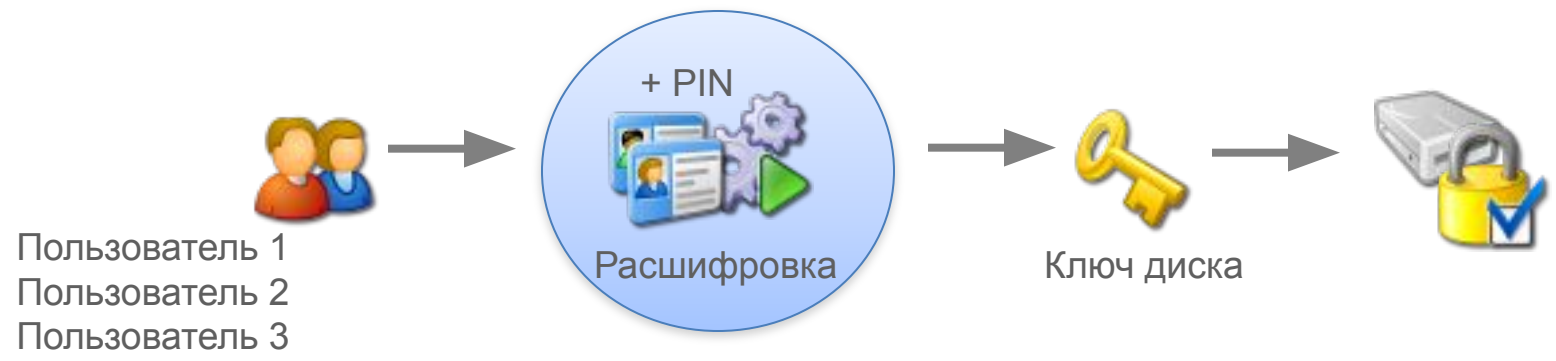
cryptopro

cryptopro HDD

Maximum

• Режим Smartcard

- ✓ Предзагрузочная идентификация с ядром Linux
- ✓ Ключ зашифрован с паролем пользователя
- ✓ Однократное введение пароля Microsoft Windows, Novell
- ✓ Многопользовательская поддержка
- ✓ Максимальная степень защиты



Security Level

Управление питанием

- Преимущество и выгода

- ✓ Более низкие расходы на электроэнергию.
- ✓ Повышение безопасности (излишняя сетевая активность)
- ✓ Определение простоев в работе
- ✓ Система раннего предупреждения проблем
- ✓ Централизованное управление и отчетность



Уничтожение данных

- Преимущество и выгода

- ✓ 100% затирание файлов, каталогов, дисков без возможности восстановления, методами:

Перезапись случайными числами

DOD (3)

DOD II (6)

VSITR (7)

Гутмана (35)

- ✓ Запланированное удаление определенных каталогов (Temp)
- ✓ Поддержка внутренних и внешних носителей



Опыт внедрения (ФКА)
2500 ПК, 4000 пользователей

Что представляет опасность?

Сотрудник предприятия может воспользоваться техническими средствами:

- Модемы
- Флэшки
- Записываемые CD или DVD диски

Внешний злоумышленник может проникнуть через несанкционированные устройства:

- Модемы
- Сотовые телефоны



Опасные устройства



15
%



70
%



15
%

Что нужно, чтобы защитить компьютеры и сеть?



1. Хороший процесс
2. Качественные программы
3. Квалифицированный персонал

Деление компьютеров по целям использования

Обычные пользователи

- Кладовщики,
- Табельщики
- Экономисты,
- Бухгалтеры,
- Руководители начального и среднего звена
- ...

2/3

Продвинутые пользователи

- Конструктора
- Программисты
- Системные администраторы
- Продавцы (маркетинг)
- Руководители среднего и высшего звена

1/3

Как построено...

- Подключение неразрешенных внешних устройств (USB-модемов и т. п.) – запрещено
- **Чтение** с флэш-накопителей – **разрешено**
- **Запись** допускается **только на разрешенные** флэш-накопители **конкретным пользователям на конкретных компьютерах**
- Разрешенные флэш-накопители маркируются наклейкой и регистрируются в журнале
- Проводится **регулярный мониторинг** событий по разрешенным пользователям и устройствам

Процесс разрешения

Руководитель
подразделения

- Определяет пользователей
- Организует приобретение носителя

Сисадмин

- приобретает носитель
- пишет записку на разрешение



Зам. ГД

- согласует записку на разрешение

Отдел
АСУП

- фиксирует носитель в базе данных
- помечает носитель наклейкой



Процесс контроля

пользователь

- подключает устройства
- копирует информацию из сети

Группа безопасности

- обеспечивает функционирование системы: фиксирование случаев подключения устройств, копирование
- анализирует информацию, копируемую из сети

Что понадобилось...

- «Положение по использованию внешних устройств и съемных носителей информации в ЛВС» и распорядительный документ
- DevicePro и хост для сервера управления (виртуальный)
- Наклейки для маркировки флэш-накопителей
- Закупка новых либо «национализация» существующих флэш-накопителей и их регистрация



- Опечатать компьютеры для исключения физического доступа

Результаты

- Сеть защищена от несанкционированного копирования информации и подключения неразрешенных устройств





Спасибо за внимание!



Cynapro Russia
426033, г. Ижевск, ул.50 лет Пионери, д.41

Tel.: +7(3412) 77-44-40
Fax: +7(3412) 48-01-05
E-Mail: office@cynapro.ru
Internet: <http://www.cynapro.ru>