

## Решения компании LANDesk® и ПК с поддержкой технологии Intel® vPro™

<b>Компания</b>	LANDesk® предоставляет интеллектуальные решения для управления процессами и безопасностью информационных систем, включающих полный спектр технологий и оборудования.
<b>Бизнес-задачи</b>	Простое управление процессами, системами и информационной безопасностью систем при минимальных инвестициях в инфраструктуру, соблюдение соответствия нормативным требованиям, а также возможность дистанционного управления и обеспечения безопасности серверов и рабочих станций.
<b>Технологическое решение</b>	ПО LANDesk® Management Suite™, LANDesk® Server Manager™, LANDesk® System Manager™ и LANDesk® Security Suite™
<b>Оборудование</b>	ПК с поддержкой технологии Intel® vPro™

### **Дистанционное управление информационными системами, аппаратная фильтрация сетевого трафика и настройка систем на базе политик безопасности**

Технология Intel® vPro™ предоставляет новые мощные аппаратные возможности программному обеспечению, предназначенному для управления системами и сетями. Решения LANDesk®, при использовании в настольных ПК с поддержкой технологии Intel vPro, значительно улучшают управление персональными компьютерами, даже если их питание выключено, операционная система не функционирует, а агенты управления не установлены. Клиенты компании LANDesk® теперь могут точнее проводить инвентаризацию ПК и аппаратных активов, сократив количество дорогостоящих визитов на рабочее место пользователей. А также эффективно контролировать соответствие их настроек политике безопасности.

#### **Современные задачи**

Сейчас перед IT-подразделениями стоит несколько серьезных задач. Первая из них – поиск всех ПК, подключенных к сети. Управление системой, которую не удастся обнаружить в сети, невозможно. Нельзя также обеспечить ее соответствие корпоративной политике безопасности, получить дистанционный доступ к системе с выключенным питанием или нефункционирующей ОС, провести инвентаризацию ее аппаратных активов, диагностику или устранение неисправностей. В этом случае для поиска неисправности, установки операционной системы или восстановления ПК требуются дорогостоящие визиты на рабочее место пользователя, что сопряжено с достаточно большими временными и денежными затратами. Одна из важнейших задач – предотвращение угроз безопасности системы, таких как вирусы, сетевые черви, общее инфицирование ПК и сокращение рисков распространения вредоносных программ по сети. IT-администраторам крайне необходимы инструментальные средства, которые позволили бы дистанционно и с большей эффективностью защищать, изолировать и восстанавливать персональные компьютеры.

## **Решения компании LANDesk®, и персональные компьютеры с поддержкой технологии Intel vPro**

ПК с поддержкой технологии Intel vPro обладают новыми аппаратными возможностями в области управления и обеспечения информационной безопасности: дистанционное включение и загрузка ОС, переадресация консоли, хранение данных об аппаратной конфигурации, аппаратные фильтры для проверки и контроля сетевого трафика.

Решения LANDesk® при использовании в настольных ПК с поддержкой технологии Intel vPro предоставляют IT-администраторам средства дистанционного управления ПК, даже если их питание выключено или ОС не функционирует. Теперь IT-специалисты могут безошибочно обнаруживать эти ПК и проводить инвентаризацию их аппаратных активов даже при отсутствии на них ОС и до установки агентов управления. После установки агента LANDesk® IT-специалисты могут гарантировать его наличие с помощью функции профилактической проверки присутствия агента. Инструментарий LANDesk® может быть более эффективным при использовании совместно со средствами технологии Intel vPro. Функция дистанционного включения позволяет IT-персоналу устанавливать исправления ПО и обновления даже на системах, питание которых в начале цикла обновления было выключено. Кроме того, решения LANDesk®, благодаря встроенным в ПК средствам обеспечения информационной безопасности, помогают техническим специалистам быстро изолировать системы, подвергшиеся DoS-атакам (отказ в обслуживании), или другим нарушениям информационной безопасности, даже, если их ОС уже поражена. Решения LANDesk®, при использовании на ПК с поддержкой технологии Intel vPro, помогают сократить дорогостоящие визиты на рабочее место пользователя, увеличить время работоспособности персонального компьютера, и повысить уровень информационной безопасности всей сети в целом.

### **Проверка активности агентов**

Существенной проблемой при управлении сетью является то, что пользователи ПК часто отключают или удаляют программные агенты, ответственные за управление системой. Для решения этой проблемы в ПК с поддержкой технологии Intel vPro имеются встроенные аппаратные генераторы контрольных сообщений и программируемые «сторожевые» таймеры, следящие за присутствием и активностью агентов. Кроме того, эти ПК оснащены каналом для дистанционных коммуникаций (его безопасность обеспечивается на транспортном уровне (Transport Layer Security) и средствами HTTP аутентификации), постоянно доступным для уполномоченного IT-персонала.

Теперь агент LANDesk® может через указанные интервалы времени связываться с сервером. Если агент пропустит назначенную проверку, ПК немедленно занесет это событие в журнал, хранящийся в энергонезависимой памяти. В соответствии с выбранной IT-политикой компьютер может сразу же направить уведомление на консоль LANDesk® об отсутствии агента. Поскольку фильтры и таймеры защищены от несанкционированного доступа, решения LANDesk®, применяемые на ПК с поддержкой технологии Intel vPro, предоставляют IT-администраторам более достоверную информацию о состоянии ПК, а так же более оперативное и более точное представление о возможной проблеме. Кроме того, IT-администраторы могут использовать решения LANDesk® для дистанционного сканирования или обновления ПК, а также для изоляции системы до тех пор, пока проблема не будет решена.

## **Дистанционное устранение проблем, даже при не функционирующей ОС**

Инструментарий LANDesk® для устранения проблем использует преимущества удаленной загрузки и средства переадресации консоли, встроенные в ПК с поддержкой технологии Intel vPro. Переадресация консоли производится при помощи контроллера SOL (serial-over-LAN). Удаленная загрузка осуществляется через адаптер IDE-R (integrated drive electronics redirect). Если компьютер пользователя не загружается, специалист службы поддержки с помощью удаленной консоли теперь может загрузить ПК с любого дистанционного устройства. Например, это может быть образ загрузочного диска, хранящийся на сетевом сервере, обеспечивающем восстановление систем. После перезагрузки ПК технический специалист сможет с помощью удаленной консоли и инструментария LANDesk® провести сеанс поиска неисправности – участие пользователя в этом процессе не требуется. Если проблема связана с программным обеспечением, технический специалист через консоль может дистанционно записать в ОС новые файлы или повторно скопировать ее образ.

Многочисленные визиты на рабочее место пользователя, обычно требующиеся для перезагрузки и повторного копирования образа ОС, теперь могут не понадобиться. Если же проблема связана с оборудованием (например, отказ жесткого диска), технический специалист сможет загрузить из энергонезависимой памяти ПК информацию о названии производителя и модели данного компонента. Затем он может записать образ системы на новый жесткий диск прямо из офиса службы технической поддержки. В этом случае потребуются только один визит на рабочее место пользователя – для установки нового жесткого диска в компьютер. Затраты на оплату труда сотрудников IT- подразделения и транспортные расходы могут быть значительно сокращены, при этом работоспособность системы будет восстановлена быстрее, и пользователь сможет возобновить работу.

### **Восстановление работоспособности инфицированного ПК**

Иногда компьютеры поражаются чрезвычайно вредоносными вирусами, такими как вирусы типа «rootkit». «Rootkit» представляет собой набор программ, которые маскируют присутствие в системе взломщика, скрывая процессы, файлы или системные данные от агентов управления и безопасности. «Rootkit»-вирусы могут добавлять новый программный код к ядру системы, подменять двоичные коды приложений и подменять или модифицировать системные вызовы. В состав этих вирусов могут также входить утилиты, способные перехватывать данные, поступающие с IT-консоли, через сетевые подключения и с клавиатуры. Например, если IT-специалист обращается к инфицированной ОС с запросом показать список всех запущенных в системе процессов, «rootkit» может перехватить этот запрос и вернуть список, который скрывает присутствие вируса, либо отключить себя во время сканирования системы. «Rootkit»-вирусы часто поддерживают рабочее состояние системы пользователя, чтобы сохранить свою активность, а IT-специалистам не всегда удается дистанционно прекратить выполнение этих процессов, чтобы восстановить работоспособность вычислительной машины. Вместо этого IT-персоналу приходится отправляться на рабочее место пользователя, чтобы восстановить ПК с помощью неинфицированного образа системы. Теперь решения LANDesk® позволяют IT-специалистам дистанционно восстанавливать ПК с поддержкой технологии Intel vPro даже в такой ситуации. IT- персонал просто использует

встроенную поддержку удаленной загрузки, чтобы заменить загрузку с собственного диска ПК неинфицированным образом системы, расположенным на восстановительном диске. (Команды выключения питания и перезагрузки, поддерживаемые ПК на базе технологии Intel vPro, являются мощной альтернативой штатным командам завершения работы ОС, которые не всегда возможно использовать).

Затем технический специалист применяет переадресацию консоли и средства просмотра системы дистанционного управления LANDesk® для наблюдения за ходом загрузки и процедурой POST (самотестирование компьютера при включении питания). После старта агента управления LANDesk®, средства дистанционного контроля и управления начинают наблюдение за процессом загрузки ОС. Это позволяет ИТ-персоналу проверять процесс загрузки ОС и обнаруживать ошибки или процессы, мешающие загрузке системы или завершению ее работы. Владея точной информацией о проблеме, ИТ-специалист может дистанционно провести очистку или перекомпоновку системы и передать ПК пользователю – все это, не выходя из офиса службы поддержки.

### **Фильтрация штатного и внештатного сетевого трафика**

Чтобы предотвратить поражение системы вирусами, ПК с поддержкой технологии Intel vPro имеют встроенные аппаратные фильтры для проверки штатного и внештатного сетевого трафика. Поскольку эти фильтры аппаратные, они защищены от несанкционированного вмешательства и не зависят от работоспособности программных агентов или всей операционной системы. Теперь с помощью решений LANDesk®, предназначенных для управления, ИТ-специалисты могут определять реакцию аппаратного фильтра на определенное поведение пакетов и условия, при которых отправляется предупреждение (и/или уведомление о событии); оно может высылаться на консоль управления даже в том случае, если ПК уже поражен. Например, решения LANDesk® с помощью этих фильтров могут обнаруживать атаки типа «flood» на ПК. В наименее опасном случае flood-атаки влияют только на производительность системы. Наихудшее последствие такой атаки – ошибки программного обеспечения, работающего с сетевым стеком. Теперь, если заданное пороговое значение числа пакетов превышено, аппаратный фильтр, определяемый решением LANDesk®, будет игнорировать пакеты, отвечающие критерию «flood»-атаки, а ПК направит сообщение с предупреждением на консоль. Решения LANDesk® могут использовать еще один аппаратный фильтр, например «фильтр LAND-атаки» для выявления пакетов с подмененным IP-адресом и установленным флагом TCP SYN. При срабатывании этого фильтра компьютер будет игнорировать все пакеты, отвечающие описанному критерию, и отправит предупреждение на консоль управления. LANDesk® обработчик предупреждений предпримет действия, определенные политикой безопасности. Аппаратная фильтрация в сочетании с мощными средствами управления LANDesk® помогает автоматизировать процессы изоляции и восстановления работоспособности системы. Например, автоматическая реакция может включать отправку электронной почты ИТ-персоналу с предупреждением о возникшей ситуации, применение политики изоляции, запуск проверки на вирусы или исполняемого файла из состава решения LANDesk®, который выполнит определенные действия по восстановлению.

### **Изоляция пораженных ПК**

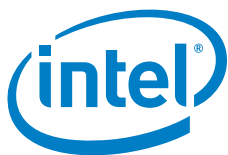
Если агент управления отключен или ПК поражен, ИТ-подразделению часто требуется быстро изолировать систему до тех пор, пока не будет обеспечено соответствие вычислительной машины политике безопасности. Теперь решения LANDesk® используют преимущества новых «изолирующих переключателей», имеющихся в ПК с поддержкой технологии Intel vPro. Этот «переключатель», предназначенный для сдерживания угроз информационной безопасности, может быть выключен встроенными аппаратными фильтрами. При срабатывании фильтра «переключатель» может отключить сетевой канал для пересылки данных, в этом случае пересылка сетевого трафика будет остановлена до того, как пакеты попадут в ОС или будут отправлены во внешнюю сеть. Кроме того, он позволит установить скоростной предел трафика, предоставляя ИТ-администратору дополнительное время для изучения угрозы информационной безопасности. Поскольку «переключатель» является аппаратным, он сохраняет работоспособность, даже если ОС поражена. Так как этот переключатель изменяет состояние программируемых фильтров, решения LANDesk® могут с его помощью реализовать гибкие средства автоматического реагирования на угрозы информационной безопасности.

### **Заключение**

Решения LANDesk® предоставляют жизненно важные средства для управления, поддержки, модернизации и восстановления ПК. При использовании в настольных ПК с поддержкой технологии Intel vPro, программное обеспечение LANDesk® значительно упрощает дистанционное управление и обеспечение информационной безопасности систем, даже если их питание выключено или ОС не функционирует. Программное обеспечение LANDesk® при использовании в ПК с поддержкой технологии Intel vPro предоставляет ИТ-администраторам широкие возможности по управлению, помогающие улучшить эффективность, снизить уязвимость сети, быстрее восстанавливать работоспособность систем, сократить простои пользователей и общие ИТ-расходы.

### **ПРЕИМУЩЕСТВА РЕШЕНИЯ**

- Улучшенные средства управления и сокращение числа визитов инженеров на рабочее место пользователя
- Фильтрация штатного и внештатного сетевого трафика на основе политик информационной безопасности
- Изоляция пораженных ПК на базе политик безопасности
- Возможность обмена информацией с ПК, даже если его питание выключено, ОС не функционирует, а агенты управления отсутствуют или отключены



### **Дополнительная информация**

ПК с поддержкой технологии Intel vPro предоставляют IT-администраторам важные аппаратные средства обеспечения информационной безопасности и управляемости, недоступные в решениях, реализованных при помощи только программных средств. Использование программного обеспечения LANDesk® позволяет IT-персоналу проводить управление и обеспечение информационной безопасности настольных систем непосредственно с информационной консоли, независимо от состояния питания ПК или работоспособности его операционной системы.

**За дополнительной информацией о ПК с поддержкой технологии Intel vPro обращайтесь на Web-сайт**

**[www.intel.com/vpro](http://www.intel.com/vpro)**

**За дополнительной информацией о решениях LANDesk® обращайтесь на Web-сайт**

**[www.LANDesk.com](http://www.LANDesk.com)**

**[www.LANDesk.ru](http://www.LANDesk.ru)**

**Ваш поставщик решений LANDesk®: ЗАО «Арбайт МЦ»  
телефон + 7 (495) 223-4322**



Копирайт © 2008 LANDesk Software Ltd., ЗАО «Арбайт МЦ». Все права защищены. LANDesk, Peer Download и Targeted Multicast являются зарегистрированными торговыми марками LANDesk Software Ltd. или ее дочерних компаний в Соединенных Штатах Америки и/или в других странах. Другие названия или бренды могут являться собственностью других сторон.