



**CYCLOPE**

**ПОЛИТИКА ДОПУСТИМОГО ИСПОЛЬЗОВАНИЯ**

версия 3.9.3.0, 18 сентября 2008

## **О политике допустимого использования (ПДИ)**

Сегодня сложно представить себе работу без компьютера. При этом всем известно, что каждый человек хотя бы раз пользовался служебным компьютером не только для выполнения рабочих задач, но и в личных целях – например, чтобы посетить какие-то не связанные с работой Интернет-сайты. Понятно, что при обширном распространении компьютерного оборудования руководители компаний ищут решения, которые помогут сократить его использование сотрудниками в личных целях. От таких решений руководители предприятий ждут повышения производительности труда, уменьшения затрат на расходные материалы, обеспечения безопасности, а в конечном итоге, и снижения общих затрат в компании.

Многие школы, предприятия и организации уже ввели у себя различные Политики допустимого использования (ПДИ), которые должны соблюдаться студентами и сотрудниками. Политика допустимого использования представляет собой свод правил, применимых к компьютерным сетям, основная цель которых состоит в формулировании ограничений на использование служебных компьютеров. К разным сетям применяются разные политики.

Недопустимое использование компьютеров подвергает компанию целому ряду рисков, включая заражение компьютерными вирусами и юридические проблемы в связи с использованием нелегального программного обеспечения. Цель Политики допустимого использования состоит в том, чтобы сформулировать правила использования компьютерного оборудования в той или иной организации. Эти правила предназначены для защиты как сотрудников, так и организации, в которой они работают.

Политика допустимого использования является неотъемлемой частью политики информационной безопасности. Часто новым сотрудникам организации предлагают подписать ПДИ до того, как им будет предоставлен доступ к компьютерной технике. Понятно, что при таком ее использовании Политика допустимого использования должна быть четкой и понятной каждому сотруднику, но при этом в ней должны оговариваться все важные требования к тому, что именно пользователи могут делать с компьютерным оборудованием в данной организации. При этом важно, чтобы в Политике допустимого использования четко оговаривались санкции за нарушение пользователем установленных норм и правил. Исполнение пользователями различных требований политики должно оцениваться в ходе регулярных проверок.

## **Проверка исполнения требований ПДИ с помощью программы по наблюдения за сотрудниками, не вторгающейся в их частную жизнь**

Компании все чаще прибегают к жестким мерам, чтобы обеспечить соблюдение политики допустимого использования сотрудниками, в частности, известны случаи увольнения сотрудников по причине неправомерного использования Интернета или электронной почты. Когда речь заходит об использовании компьютеров на рабочих

местах, руководители компаний чаще всего беспокоятся о посещении тех или иных веб-сайтов: в 76% компаний контролируется активность сотрудников в сети Интернет (согласно последнему исследованию AMA/ePolicy, посвященному политикам и процедурам контроля поведения сотрудников на рабочих местах). При этом в 65% компаний используются различные программные средства, которые блокируют доступ к избранным сайтам.

Мониторинг деятельности сотрудника с использованием компьютера принимает самые разнообразные формы:

- в 36% компаний контролируется происходящее на экране, вводимый с клавиатуры текст и время, которое сотрудник работает с клавиатурой
- в 50% компаний принято просматривать файлы, с которыми сотрудники работают на своих компьютерах
- в 55% организаций существует практика проверки сообщений, отправляемых по электронной почте

Из тех компаний, которые занимаются мониторингом деятельности сотрудников, в 80% компаний сотруднику сообщают о том, что его деятельность с клавиатурой отслеживается, в 82% компаний сотрудник узнает о том, что в компании принято просматривать его файлы, в 86% случаев его проинформируют о контроле электронной почты, а в 89% случаев он узнает и о том, что использование им Интернета контролируется.

Озабоченность возможными судебными разбирательствами, а также роль, которую играют в них электронные носители информации, заставляет все большее количество компаний формулировать и применять свои политики по использованию компьютерных технологий. В разрабатываемых Политиках допустимого использования компании устанавливают правила по использованию в личных целях электронной почты (84%), Интернета (81%), программ для обмена мгновенными сообщениями (42%), по ведению личных сайтов в рабочее время (34%), по размещению личных сообщений на корпоративных блогах (23%), а также по ведению личных блогов в рабочее время (20%). Электронная почта, мгновенные сообщения, посещаемые веб-сайты – все это становится объектом внимания компании.

Производители программного обеспечения предлагают самые разнообразные решения для наблюдения за деятельностью сотрудников – от агрессивных программ, таких как клавиатурные шпионы, которые отслеживают ВСЮ деятельность на компьютере, до комплексных решений, которые предоставляют руководству информацию о деятельности сотрудника или целого отдела, не вторгаясь при этом в частную жизнь сотрудников.

Cyclope – прогрессивное программное решение, которое отслеживает деятельность сотрудников на компьютерах и позволяет руководству оценить ее эффективность, сохраняя при этом за сотрудниками право на неприкосновенность частной жизни. Cyclope предоставляет сотруднику, ответственному за информационную безопасность в организации, все отчеты, необходимые для проверки соблюдения сотрудниками Политики допустимого использования. Основные функциональные возможности Cyclope:

- **Использование приложений:** отображаются все запускаемые пользователем приложения, в том числе и те, использование которых противоречит ПДИ. Показывается также продолжительность работы с приложениями и доля их использования в общем рабочем времени. Понятно, что должностные инструкции каждого сотрудника дают достаточно точное представление о том, какие именно приложения нужны ему для работы, и разделить используемые приложения на продуктивные и непродуктивные. Сформированный график даст руководителю понять, пользовался ли сотрудник продуктивными приложениями или играл в компьютерные игры. Кроме того, директор по информационным технологиям может также выявить и случаи использования нелегальных приложений, которые могут привести к судебному преследованию компании или нарушению безопасности в компьютерной сети. Контролируется также внедрение вредоносных программ (вирусов, червей, троянских программ и т.п.) в сеть или на сервер. Также в отчетах будут видны такие приложения, как клиенты для обмена мгновенными сообщениями, бесплатная электронная почта (используемая в личных целях), клиенты для обмена файлами. Cyclope осуществляет мониторинг используемых приложений, позволяя системным администраторам контролировать приложения, работающие на том или ином компьютере, видеть, насколько корректно используются компьютеры, а также понимать, где нужно ввести дополнительные машины.
- **Активность пользователей:** Cyclope предоставляет информацию об активности сотрудника (статистика по времени активности и времени простоя), а также позволяет сравнить производительность труда разных сотрудников, работающих на одинаковых должностях.
- **Интернет и чаты:** Часто происходит так, что сотрудники проводят большую часть времени, посещая Интернет-сайты или общаясь с друзьями с помощью программ обмена мгновенными сообщениями. Cyclope предоставляет точную статистику относительно того, какие именно Интернет-сайты посещал сотрудник, а также сколько времени он провел на каждом из них (можно будет увидеть и посещение сайтов, которые запрещены Политикой допустимого использования). Отслеживаются также и имена собеседников сотрудника в различных программах обмена мгновенными сообщениями, но не записываются сами сообщения, что соответствует принципу невмешательства в частную жизнь сотрудников.
- **Работа с документами:** предоставляется подробная информация относительно того, какие документы создавались или открывались сотрудником, а также сколько времени он работал с тем или иным документом.

### Конфиденциальность и законодательство

Cyclope придерживается принципа конфиденциальности частной жизни. При работе приложения остается неприкосновенной частная информация сотрудника и не перехватываются сообщения, что не мешает Cyclope отслеживать, чем именно занимается сотрудник на работе, соблюдает ли он должностные инструкции и правильно ли он использует свой компьютер.

В соответствии со статьей 23 Конституции Российской Федерации каждый гражданин РФ имеет право на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений, ограничение которого допускается только на основании судебного решения. Следовательно, руководитель компании, принимающей к рассмотрению вопрос о внедрении решения для контроля персонала, должен учитывать необходимость соблюдать конфиденциальность частной жизни сотрудников, и применять соответствующие решения, которые не будут выходить за пределы допустимого контроля. На сегодняшний день Cyclope является единственным на российском рынке решением по мониторингу активности сотрудников, разработанным и функционирующим в соответствии с законодательством РФ.

### **Заключение**

Проверка соблюдения сотрудниками Политики допустимого использования направлена на следующие аспекты деятельности, контролируемые приложением:

- использование сети Интернет
- недопустимое использование нелегальных материалов
- недопустимое использование оборудования компании (принтеры, сканеры и т.п.)

Функции мониторинга и составления отчетов программы Cyclope предоставляют информацию, необходимую для оценки выполнения сотрудниками Политики допустимого использования. Предприятие, внедрившее Политику допустимого использования и инструменты для контроля за ее соблюдением, может рассчитывать на значительное повышение эффективности труда, а также информационной безопасности в компании.