Этика

Принцип согласия, основанный на информации, врачи администраторы систем аналогичен. Врачи информируют пациентов о вариантах лечения, их достоинствах, недостатках и вероятности успеха. Пациенту предоставляется возможность принять или отклонить лечение без давления. Однако, если кто-то не может понять информацию или не может дать согласие, например в случае комы или отсутствия близких родственников, соблюдаются определенные условия. Процедура должна быть успешной, учитываться интересы пациента и использоваться все возможности для получения согласия. Нарушение принципа согласия на основе информации является крайней мерой. Эти принципы применимы и к системным администраторам. Необходимо, чтобы люди понимали правила, по которым они работают. Соглашение об уровне обслуживания, например, может содержать информацию о рабочих часах и уведомлении клиентов о перезагрузках серверов. SLA помогает клиентам понять, как будет работать системный администратор в различных ситуациях.

Этический кодекс системного администратора:

1. Соблюдение профессиональных норм на работе и отсутствие предвзятости.
2. Честность, открытость к критике и восприятие ошибок как возможности для улучшения.
3. Избегание конфликтов интересов и убеждений.
4. Ограничение доступа к личной информации только для выполнения технических обязанностей и поддержание ее конфиденциальности.
5. Изучение и соблюдение законов и политик, связанных с работой.
6. Коммуникация с руководством, пользователями и коллегами для обсуждения компьютерных вопросов.
7. Обеспечение целостности, надежности и доступности систем.
8. Постоянное образование и обмен знаниями с другими.
9. Сотрудничество с компьютерным сообществом для поддержания целостности сетевых и компьютерных ресурсов.
10. Вклад в разработку политик и правил, соответствующих этическим принципам.

Некоторым пользователям нужен привилегированный доступ для работы. Такой доступ позволяет писать и отлаживать драйверы устройств, устанавливать программы для других и выполнять другие задачи, требующие прав администратора. Организации должны установить правила поведения для таких пользователей, чтобы предотвратить злоупотребление привилегиями. Эти правила должны включать следующее:

1. Пользователь должен использовать привилегированный доступ ответственно.
2. Пользователь должен использовать высокие привилегии доступа только при необходимости по работе.
3. Компания должна предоставить процедуры для минимизации ущерба, связанного с возможными ошибками, например, делать резервные копии перед внесением изменений.
4. Должны быть процедуры для действий в случае, если пользователь получает информацию, к которой не должен был иметь доступ. Более конкретно, пользователь должен знать, как поступить в случае обнаружения нарушений, например, сообщить руководству.
5. Правила поведения должны также указывать, что делать, если пользователь получает важную информацию о компании, которая не является преступлением.
6. Последствия ошибок должны быть четко описаны. Ненамеренные ошибки не должны наказываться, если о них было своевременно и честно сообщено.

7. Сотрудники с привилегированным доступом должны подписать расписку о прочтении правил поведения. Эта расписка должна быть храниться у руководителя или в отделе кадров.
8. Группа системных администраторов должна отслеживать, у кого есть привилегированный доступ к системам. Это позволит своевременно отключать доступ для уходящих пользователей.
9. Политика использования привилегий должна регулярно пересматриваться и может предусматривать автоматические напоминания о необходимости подписания повторной расписки.

В организациях необходимы политики соблюдения авторских прав для сотрудников. Компании должны избегать использования пиратского программного обеспечения из-за финансовых обязательств и негативного общественного мнения. Рейды организаций по борьбе с компьютерным пиратством также являются неприятными и нежелательными. Поэтому необходимо использовать только лицензионное программное обеспечение и не допускать установку пиратских программ. Чтобы решить проблему неправомерного использования программ, политика должна содержать примеры распространенных нарушений и требовать правильного приобретения и использования программного обеспечения. Некоторые компании также наказывают сотрудников за установку программ без одобрения руководства, а указание программ, которые можно свободно загружать, может сделать политику более понятной и удобной для всех сотрудников. Это поможет предотвратить использование нелицензионных программ.

Соблюдение политики легко обеспечить, покупая программы с лицензиями и устанавливая их на все рабочие станции. Это избежит нарушения правил. Если необходимо, требуйте при покупке новых рабочих станций или серверов включать операционные системы и приложения или лицензии на них. Бесплатное и открытое программное обеспечение позволяет копировать, если не запрещается лицензией. Важно изучить лицензию, если сотрудники изменяют исходный код. Правду о нарушении авторских прав нужно сообщить и убедиться, что эта политика до всех доведена. Системным администраторам особенно важно это понять. Установление политики неприкосновенности личной информации и мониторинга является важным этическим вопросом. Ожидания сотрудников в отношении неприкосновенности личной информации нужно формировать, чтобы избежать неправомерных действий, вызванных их незнанием правил. Распространение политики и напоминание о ней должны быть постоянными. Компании могут требовать от сотрудников давать расписки о прочтении политики, а также переиздавать положения о неприкосновенности личной информации через сводки новостей или бюллетени. Краткое содержание политики может быть размещено на видном месте или на экране входа в систему для большей эффективности. Неинформирование сотрудников о правилах неприкосновенности личной информации может привести к риску для бизнеса, так как пользователям неизвестны потенциальные угрозы, связанные с их действиями. Также необходимо учитывать различные законы о неприкосновенности личной информации в разных странах при ведении международного бизнеса. Формирование ожиданий также помогает поддерживать репутацию системных администраторов и избежать недопонимания и недоверия со стороны пользователей.