

Москва

май-август 2006

Алексей Барабанов <alekseybb at mail dot ru>.

В поисках профессиональной этики сисадминов.

В Интернете и печатных изданиях можно встретить множество документов, описывающих разнообразные представления о принципах системного администрирования. Попробуем найти в этих вариантах общие черты и определить направление совершенствования.

Формирование профессии системного администратора тесно связано с созданием общих представлений о принципах деятельности сисадминов. Такие принципы, безусловно, должны опираться на технологические особенности профессии, но создавать стойкую и непротиворечивую систему этических норм, независимую от уровня развития технологии. О необходимости таких принципов задумывался любой автор, добросовестно подходящий к процессу описания системного администрирования. Например, широко известно «толкование от Эви Немет». В нашей стране познакомились с ним по переводу второго издания руководства системного администратора [1] от группы авторов под предводительством этого специалиста. И, хотя далее Эви Немет опубликовала много литературы на данную тему [2], отслеживая изменение среды и спроса, но разделы, посвященные «вечным вопросам», почти не менялись и путешествовали из издания в издание. Поэтому оказалось, что принципы деятельности сисадмина Linux, согласно изданию 2002 года [3], буквально повторяют морали от 1995 года [1]. Быть может, авторы нашли то самое, что уже более не совершенствуется? Предполагаю, что нет! Эви Немет и компания были проповедниками подчинения деятельности сисадминов корпоративной политике. А признаком зрелости профессии является создание независимой системы профессиональных норм. Например, таких, что регламентируют деятельность адвокатов, врачей и даже бухгалтеров в развитых странах!

Когда пытаются рассмотреть данную проблему, то, как правило, рассуждают со стороны некой абсолютной и абстрактной правды или социального заказа. Например, чтобы автомобиль доехал из точки А в точку В с оптимальной скоростью, рассматривают, сколько надо залить бензина, как надо «давить» акселератор, какого качества должно быть дорожное покрытие, и никто, подчеркиваю – никто! - не пытается рассмотреть данную проблему с точки зрения «самого» автомобиля. А «ему» лучше вообще никуда не ездить, а стоять чистеньким в гараже. Так и с системным администрированием, все варианты рекомендаций созданы явно с подачи заказчиков. Причем, трансформация произошла незаметно. Началось все с книжек, подобных пресловутой серии «библей» от Эви Немет. Затем идеи сортировки сисадминов по методам ведения работы на «бандитов», «фашистов» и «идиотов» проникли в массовое сознание [3]. И завершилось все вполне официальным бойскаутским катехизисом [5] от Red Hat Inc., претендующим на истину в последней инстанции. Но представители профессиональной группы тоже имеют свои интересы и тоже могут нуждаться в защите. Этот вопрос также должен регулироваться прозрачным образом.

Получается, что и требования общества к представителям профессии, и претензии самих профессионалов должны получить некоторое формальное выражение и закрепление в виде соглашения. Со стороны общества такое закрепление создается признанием норм

поведения профессиональной группы и поддержкой этих норм, выраженной законодательно.

Конечно, в рамках одной журнальной статьи невозможно решить эти вопросы. Здесь лишь попытаюсь определить направления формирования такой системы норм или профессиональной этики, начиная с книг Эви Немет, и завершая другими публикациями, и поставлю задачи, не нашедшие отражения в указанных работах.

Примитивная корпоративная этика.

Вопросы общего характера в трудах Эви Немет и команды рассматриваются в самом начале, как «основные задачи системного администратора», и ими же завершаются книги упомянутого «сиквела», это глава «Стратегия и политика». Иногда заголовки варьируются, но общая схема повторяется с педантичностью плана школьного сочинения: введение в профессию, основной блок «технических аргументов», и заключительное напутствие.

Учитывая хронологию и некоторые положения этих материалов, отнесу их к начальному этапу осмысления профессиональной этики. Даже «основные задачи» представляют собой просто набор абстрактных пожеланий работодателя. Вроде того, что бы Вы хотели от сисадмина, но стеснялись это попросить. Авторы постоянно сбиваются на бытовые примеры и случаи из университетской практики самозаявленных админов. И временами откровенно признаются, что описывают предмет с позиции новичка: «Вы можете обнаружить, что системное администрирование Вам нравится, и захотите стать штатным администратором.»[1, раздел 1.6]. Забавно, что и к публикации семью годами позже [3, раздел 1.9] авторы снова в нерешительности и буквально слово в слово повторяют совет. За семь лет можно бы и определиться с выбором профессии!

Итак, рассмотрим, как специалистами под руководством Эви Немет понимаются принципы деятельности системных администраторов. Буду исходить из того, что Вы имеете возможность ознакомиться с подлинниками [2] и здесь стану отмечать только важные с моей точки зрения или примечательные положения.

Прежде всего, авторы используют эмпирические и экспертные правила. Самые сильные аргументы: «мы беседовали с видными деятелями в области системного администрирования...» и «мы знаем одну фирму...». Но, в целом, оперирование интуитивно понятными истинами и бытовыми рецептами (всем известный конверт с паролем суперпользователя) дает достаточно ясную картину ошеломленного человека, который только-только разобрался с проблемами и спешит поделиться своими рецептами. Особо трогательно упоминание авторов о том, как «машины другого факультета инфицировали весь университетский городок». Вот проблема-то! К чести авторов, они не повторили этот же пример в версии [3]. Вообще, в [3] практически нет примеров из университетской практики. Хотя, быть может, дело в элементарном взрослении и смене места работы.

Но даже на таком примитивном материале Эви Немет сотоварищи сделали ряд очень важных замечаний, которые нельзя не процитировать и прокомментировать:

...Вы ...захотите стать штатным администратором. ...проблем с поиском работы у Вас не будет. Но отношения с коллегами и руководством ... обязательно обострятся. [1, 1.6]

Это фактическое признание, что сисадмин является участником обычного сервисного антагонизма. В версии [3] оно отсутствует, так как там уже декларируется подчинение сисадмина корпоративной политике, а внутри корпорации антагонизм неприемлем, так как там царит «тимбилдинг» (team building – методика сплочения коллектива).

Ответственное лицо должно иметь диктаторские полномочия. [1, 32.2]

Конечно, это в адрес сисадмина в период ликвидации проблемы. В поздней версии [3] снова отсутствует. Ну, какая диктатура может быть в устоявшейся корпоративной иерархии?

Вышестоящее руководство часто не имеет ни малейшего представления о том, чем занимаются системные администраторы. [1, 32.8]

Данное положение в [3] еще более усугублено. Раздел «Как руководить руководителями» стал короче, но наполнился конкретными замечаниями и выводами. Например, в число непонятливых руководителей добавлены «менеджеры нетехнического звена».

Удваивайте или утраивайте время, которое, на Ваш взгляд, понадобится для решения ... задач. [1, 32.8]

Очень важное положение, присутствующее и в [1] и в [3]. На мой взгляд, это меткое замечание, вместе с предыдущим предложением, подчеркивает, что сисадмин обязан действовать исходя из профессиональных, а не общепринятых взглядов на его работу. Эви Немет оправдывает это профессиональными рисками. Логика совершенно прозрачна. Поскольку никто не имеет представления о сути работы сисадмина, то в случае неудачи он рискует необъективным расследованием. Если же работа пройдет «гладко», то по той же причине никто не усомнится в оценке трудозатрат.

Системные администраторы ... часто забывают, что они – поставщики услуг, а пользователи – их клиенты. Многие администраторы втайне считают, что системы принадлежат им... [1, 32.9]

Дословно повторено в [3]. Ну, естественно, надо же показать сисадмину, что все кругом не его, а вот сам он всем окружающим полностью обязан. Очень напоминает: все, что твое, то общее, а вот что общее, то уже не твое. Но обратный вывод, что сисадмин обязан компании лишь в меру оплаты его услуг, почему-то авторы забыли сделать!

В продолжении этой мысли авторы возвращаются к тому, что им трудно определить кто же прав в решении вопросов типа «сисадмин vs наниматель» и признаются:

Некоторые качества хорошего системного администратора противоречат друг другу. [1, 32.9]

В [3] прояснение так и не снисходит к ним, и авторы снова повторяют это высказывание буквально.

Далее, замечание, на первый взгляд, совсем не по теме этики и морали:

Что делает резервная копия? Надежно нарушает защиту файла. [1, 32.14]

Это самое парадоксальное экспертное мнение, процитированное в [1]. В версии [3] отсутствует. Вероятно, администраторы linux-систем не занимаются резервным копированием, по мнению Эви Немет и компании. Но нам интересно это высказывание, так как оно признает, что даже в повседневной деятельности сисадминов постоянно складываются ситуации, ломающие общепринятые стереотипы (в данном случае стереотипы безопасности).

Но, вместе с тем, в [3] возник ряд новых утверждений:

...администратору необходим доступ к копиям важных данных, находящихся в компьютерах и на внешних носителях. [3, 29.2]

Иначе говоря, сисадмин тем эффективнее работает, чем меньше ограничений в доступе он имеет.

Системные администраторы обычно не отвечают за то, что пользователи хранят на своих компьютерах. [3, 29.3]

Хорошо подмечено. Если развить эту мысль, то системные администраторы не могут отвечать за процесс работы пользователей, в результате которого образуются те самые данные, за которые они не отвечают. Но чуть далее уже не так лаконично авторы выворачивают все наизнанку, доказывая, что:

...чем больше вы контролируете использование Internet-ресурсов, тем большую ответственность несете за действия пользователей. [3, 29.3]

И уж совсем непоследовательно группа авторов с Эви Немет во главе высказывается в отношении нелегального копирования программного обеспечения. Там даже нельзя процитировать твердую рекомендацию. Просто отсутствует конкретная фраза, которая точно описывает авторскую позицию. Вместо этого какие-то бесхребетные поучения:

...помните, что речь идет о вашей личной и профессиональной честности. [3, 29.3]

Хотя, если следовать предложенному ими же принципу разделения ответственности, то сисадмин не должен отвечать за копии ПО, нарушающие лицензии. Но авторы здесь требуют от сисадминов вопреки всякой логике «стучать» на своих клиентов.

Использование термина «этика» в [1] можно заметить, но и только. В контексте раздела «Военные истории и этика» первое с избытком, а второе лишь как синоним балластной морали. А вот в [3] уже специально объяснена авторская позиция:

Невыдуманные истории и этика поведения. При чем здесь этика, спросите вы? Дело в том, что в работе системных администраторов многое строится на доверии. [3, 29.8]

Вот оно как! То есть, этика есть, но как набор моральных норм, укрепляющих доверие к ... К чему же? И далее Эви Немет поясняет:

Администратор должен соблюдать конфиденциальность информации, с которой работают пользователи, и защищать профессиональные секреты компании. [3, 29.8]

Ну, вот и проговорились - все-таки интересы компании в первую очередь! И это на фоне того, что сисадмин не несет ответственности за содержимое пользовательских компьютеров, с одной стороны, и обязан доносить о нарушении лицензий, с другой! Прямо каша какая-то! Уму не постижимо, как выполнить все рекомендации хитроумной Эви Немет и ее суматошных соавторов.

В заключение можно только порадоваться, что работы [1,3] созданы выходцами из академической среды, а не искушенными последователями Хаббарда. И поток поведенческих рекомендаций, выработанный в локальных сетях кампусов, не такой уж большой. Но обращаю ваше внимание, как на авторов давит необходимость сделать реверансы в пользу их корпоративных работодателей.

Народные представления.

Вне всякой зависимости от литературной версии самоосознания сисадминского профессионализма, в представлениях окружающих, да и в самой среде системных администраторов, тоже зарождались некие зачатки стереотипов поведения. Но только не в виде моральных кодексов, а в виде всяких фольклорных форм, например, анекдотов. Но самое лучшее, наиболее полное и, несомненно, известнейшее воплощение этого принадлежит перу Стефана Зелински [4]. Отечественные любители «сетевого юмора» знакомы с переводом [5], который чуть короче оригинала. В этом произведении рассматривается в утрированной форме поведение 4-х типов системных администраторов, отличающихся этическими установками и, соответственно, мотивацией.

Технический бандит, администратор-фашист, маньяк и идиот последовательно попадают в типичные производственные ситуации. Каждый действует в силу собственных убеждений и привычек. По замыслу автора, ни один не добивается успеха. На этом и построен комизм положения. То есть тут должен содержаться определенный юмор. Но, увы, не всегда именно тот, что планировал автор. И возможно, при детальном рассмотрении в этом замечательном произведении оказывается еще более оснований для смеха.

Несмотря на желание автора высмеять методы администратора-фашиста, наряду с остальными, очень часто именно его действия происходят в рамках ожидаемого и именно они оказываются более успешными, чем действия остальных. Рассмотрим выборочно несколько типовых ситуаций из [5].

Ситуация 1. Нехватка дискового пространства.

Технический бандит погружается в пучину исследований и прогнозов. Маньяк просто удаляет самые большие файлы. Идиот самые большие файлы пытается упаковать. А вот админ-фашист: «Активно пользуется квотированием диска.» Автор пытается перевернуть ситуацию: «Не допускает никаких исключений, чем полностью останавливает деятельность разработчиков». То есть, в этом случае разработчики настолько слабоумны, что не реагируют на сообщения операционной системы. Возможно, ситуация взята из практики.

Ситуация 4. Авария загрузочного диска.

Технический бандит совершает чудеса и восстанавливает все сам. Маньяк сводит все к скандалу. Идиот не замечает ничего. А вот админ-фашист: «Начинает расследование аварии...» То есть делает то, что и требуется. Кстати, предложения в [3] наиболее близки действиям администратора-фашиста.

Ситуация 5. Слабая производительность сети.

Технический бандит опять занимается какой-то самодеятельной модификацией. Маньяк просто размыкает кабели. Идиот делает нечто непотребное. А вот админ-фашист снова на высоте: «Звонит в Беркли и AT&T, приставая к ним, как установить сетевые квоты. Пытается уволить поклонников игры в xtrek.» Правилам работы в сети Эви Немет посвящает в [3] целый раздел. Нет нужды повторять, что использование сети для игр они не предусматривают.

Ситуация 6. «Глупые» вопросы пользователей.

Технический бандит просто издевается над чайниками. Маньяк ведет себя как идиот из ситуации 5. Идиот увлекается панибратством. И снова админ-фашист делает практически то, что может привести к успеху: «Блокирует вход пользователя в систему, пока тот не представит веские доказательства своей квалификации». Эви Немет в [3, раздел 29.2] предлагает не допускать к работе пользователей, пока они не согласятся с правилами использования. Если предполагается осознанное согласие, то оно подразумевает наличие квалификации, достаточной для понимания и применения правил.

Ситуация 7. Установка новой операционной системы.

Технический бандит ведет себя как типичный пользователь Gentoo. Маньяк просто всех выкидывает из системы. Идиот копирует дистрибутивный диск в ядро. А админ-фашист: «В первую очередь изучает законодательные акты против производителя, поставляющего программное обеспечение с ошибками». Ну, разве это не разумно?

Раскроем карты, как же Стефан Зелински определил типаж администратора-фашиста - «Обычно законченный тунеядец, вынужденный заниматься администрированием системы». Очень мило! Это так типично для сисадмина. Ведь не даром лень считается добродетелью системного администратора. Похоже, Стефан Зелински попал прямо «в яблочко», совсем не целясь. Он умудрился указать самый правильный стиль поведения сисадмина! Хотел посмеяться, но вместо этого научил!

Изощренная корпоративная этика.

Но, безусловно, всех превзошли гуру из Red Hat Inc. С русским переводом последней версии можно ознакомиться в [6]. Наиболее старый из размещенных в Сети оригиналов можно найти по адресу [7] и определить, что они слабо эволюционируют. Конечно, можно предположить, что мнение специалистов Red Hat Inc. являет собой наиболее свежий и, значит, наиболее верный взгляд на обсуждаемый предмет. Но на деле это не так. Требования не только много раз продублированы, но и часто противоречат одно другому. Общее впечатление таково, что авторы стремились не оставить сисадмину никаких шансов уклониться от выполнения придуманных ими обязательств. Далее буду по-порядку анализировать каждое утверждение «Философии системного администрирования» от Red Hat Inc.

1. Автоматизировать все, что можно.

Естественно, не нужно понимать буквально. Безусловно, не в силах сисадмина автоматизировать все. Но даже с такой поправкой - «уступайте старикам, помогайте женщинам» - данное правило не приемлемо. И оговорка, мол, поищите сначала решение в Интернете, тоже ничего не меняет. Это правило фактически призывает системного администратора заняться несвойственной ему работой в стиле «технического бандита» Стефана Зелински [5]. Задумаемся, чем же должен заниматься сисадмин, и кто он такой вообще? Во-первых, сисадмин - это нанятый сотрудник, а, во-вторых, он должен обслуживать эксплуатационный цикл информационных систем (далее ИС), и не более! Создание новых сущностей или объектов своей работы не входит в его задачу. Даже самое первое обоснование «любое задание, возникающее более одного раза» надо считать вздорным! В работе системного администратора не возникает никаких заданий. Вся его работа подчинена и полностью обусловлена возможностями программного обеспечения и аппаратуры. Что значит, далее цитирую из [6], «возникло более одного раза» и, чуть далее, «проверка свободного дискового пространства»? Это откровенный бред! Или в эксплуатируемой ИС предусмотрена данная отчетность, или нет. Не может руководство ВДРУГ поставить такую задачу. И не может сам системный администратор, однажды проснувшись, ВДРУГ озаботиться данной проблемой. Но все проясняется далее. Цитирую: «функции, связанные с деятельностью компании», и, самое смешное, «загрузка новых данных на веб-сервер...». Вот и итог развития подобной ущербной логики. Сисадмина превращают в «палочку-выручалочку», в дополнительного сотрудника рекламного отдела или в аварийного бухгалтера. Вы этого хотите? Я – нет!

Итак, сисадмин должен заниматься эксплуатацией, а не автоматизацией. Вся автоматизация должна рассматриваться как отдельная задача. И на период выполнения этой задачи системный администратор становится разработчиком. Теперь задумаемся. Если наниматель оплачивает работу сисадмина, исходя из 100% занятости, то сисадмин-разработчик или осуществляет свою внедренческую деятельность за свой счет, или в ущерб основной работе. Третьего не дано! Следовательно, какая-либо автоматизация не входит в обязанности сисадмина. Все работы по модификации ИС должны оплачиваться отдельно и, возможно, даже как отдельный проект, с привлечением субподрядчика.

Таким образом, исключая примитивное скриптостроительство, сисадмин не должен заниматься никакой автоматизацией! Если же в вашей практике возникает подобная необходимость, рассматривайте ее как модернизацию системы. Если сисадмин, Ваш подчиненный, занят этим, значит, в первоначальной спецификации ИС есть ошибки.

2. Документировать все, что можно.

Здесь вздорность видно даже невооруженным глазом. Внимательный читатель должен и сам заметить, что такая постановка задачи есть следствие из только что обсужденного заблуждения. Ибо, когда возникает проблема документации? Только тогда, когда сисадмин выполнил нештатную модификацию. И только в этом случае он должен задокументировать ее, так как все ординарные действия уже описаны в руководствах, сопровождающих ИС и ее компоненты.

Более того, если задуматься, то процедура документирования, как сугубо ручной процесс, в корне противоречит принципам эксплуатации автоматизированных систем. Вопрос нужно

ставить так, что ИС должны обладать свойствами самодокументирования. Например, из предыдущего тезиса - «проверка свободного дискового пространства», если такой параметр протоколируется, чем данные отчеты не документация? Ведь, можно рассматривать некий мониторинг, а можно и задокументировать моментальное значение выбранного параметра.

Таким образом, если ИС строится по устойчивым индустриальным и корпоративным стандартам, то не возникает никаких проблем, требующих нештатного документирования. То есть, документировать надо лишь, что НУЖНО. В противном случае неверно выбрано программное обеспечение, требующее неординарной настройки, или принят на работу бездарный сисадмин, выполняющий все работы одному ему ведомым способом. Не знаю, что хуже. Вероятно, надо учитывать, что будет дороже!

3. Общаться как можно больше.

Это самый смешной раздел! В глазах всех пользователей - сисадмин, в лучшем случае, «домовой из аппаратной». В глазах сисадмина - пользователи, в лучшем случае, назойливые источники проблем. Рассказывать пользователям о структуре системы или не безопасно, если они вездливые, или бесполезно, во всех остальных случаях. Вообще глупо это делать заранее. У нормального сисадмина должно хватать время только на ответы, а никак не на инициативные лекции. В анализе рассматриваемого тезиса возникает сильное ощущение, что авторы спутали пользователей и заказчиков. Причем, это не описка, это системная ошибка, так как, оказывается, у данной идеи есть еще и подпункты, детализирующее это заблуждение. Рассмотрим их в том же порядке.

3.1. Рассказывайте пользователям, что вы собираетесь делать.

Если выполняется плановая операция, то надо не рассказывать, а предупреждать, иначе выполняется операция по запросу пользователя и в рамках штатных обязанностей сисадмина, и, значит, опять же не о чем рассказывать. Да и что может быть вздорнее, чем болтливый и «липучий» сисадмин? Ну, разве что генерал, бегущий вприпрыжку в мирное время!

Хотя, быть может, я что-то не так понял. И авторы опуса на самом деле предлагают иное. Цитирую: «отдел бухгалтерского учёта испытывает трудности с сервером базы данных, который временами очень медленно работает. Вы планируете остановить сервер, заменить процессорный модуль на более мощный...». Да нет, все верно! Полный вздор! «Перевозу» процитированное: отдел бухучета ЗАПЛАНИРОВАЛ модернизацию оборудования; для этого была запланирована модернизация сервера; для чего был куплено новое оборудование; и это все прошло массу согласований, начиная с финансовых и кончая процедурными... Вам все еще кажется, что сисадмин должен прийти в бухгалтерию и рассказать о запланированной модернизации? Есть маленькая разница между «рассказать» и «известить». Согласитесь, что «известить» не укладывается в категорию общения. Это ближе к командному наречию. Именно тому, к которому в реальной практике общения и приходится прибегать.

Но кое-что верно подмечено. Здесь авторы не могли не признать, что следует максимально оградить пользователей от ненужных им технических подробностей. Сформулируем наш подход в данном вопросе: надо всеми возможными способами ограничивать интерес пользователей к операциям обслуживания ИС. Почему? Если вы практикующий сисадмин, а не теоретик, то легко догадаетесь: они никогда не должны иметь возможность

использовать служебную информацию о действиях сисадмина, чтобы списать на него свои проблемы!

3.2. Рассказывайте пользователям, что вы делаете.

Здесь уже применяется суггестивная технология для закрепления рефлекса подчинения сисадмина. Подумал – рассказал, приступил к работе – продолжай болтать непрерывно! Можно в ответ повторить контраргументы из предыдущего раздела, чтобы закрепить процесс антивнушения.

3.3. Рассказывайте пользователям, что вы сделали.

Ошибка очевидна. Безусловно, все модификации должна описываться. Безусловно, все работы должны протоколироваться. Но не в качестве темы для бесед с пользователями (вспомните панибратствующего «маньяка» из заметок Зелински), а именно в том смысле, как это рекомендует Эви Немеет. Информировать руководство о том, что собираетесь делать, что делаете, и что сделали. Для чего? Дословно из [3, 29.6]: «...если необходимо собрать аргументы в пользу найма дополнительного персонала или покупки нового оборудования.», и, чуть далее, «он (документ – А.Б.) может стать серьезным оружием в ежедневных разборках.». Замечаете, как изменился контекст работы сисадмина от описанного в работах Эви Немет до того, что существует в грезах инженеров из Red Hat Inc. Задумайтесь, что вам ближе?

4. Знать свои ресурсы.

Вот снова элемент внушения. Если, следуя рекомендации выше все задокументировано, и даже, как предложено далее, несколько раз произнесено вслух публично, то что еще нужно? Быть может, продекламировать перед сном? Или, возможно, этап документирования, по логике Red Hat Inc., может производиться в ситуации, когда предмет работы сисадмина и собственно объект документирования ему известен не полностью? Ну а финальное заклинание вообще трудно понять: «Отсутствие “ситуационной осведомленности” в отношении доступных ресурсов часто хуже, чем полное отсутствие осведомленности». «Покрутил» это как конфетку, ничего не понял! Быть может так: «полное отсутствие осведомленности заведомо лучше, чем отсутствие осведомленности в конкретной ситуации»? Очень напоминает поведение «идиота» в описании Стефана Зелински. Неужели в Red Hat Inc. хотели именно такого?

5. Знать своих пользователей.

Загадочное требование. Если сисадмин знает свои ресурсы, все задокументировал, и все начитал каждому пользователю, то неужели можно предположить, что он еще не познакомился с каждым из них? А! Быть может надо узнать их приватные данные? Жены, дети, домашние любимцы... Вероятно именно так, поскольку подчеркивается «как вы сможете понять, какие системные ресурсы нужны пользователям, не понимая самих пользователей?» Задумаемся, в каком случае возможна ситуация непонимания пользователей? Если пользователи слышали инструкции, прочли документацию, то непонимание может иметь источник только в неформальном аспекте. Тут мудрецы из Red Hat Inc. впервые затрагивают этику. Они извиняются, что употребляют вообще такой термин как «пользователи», но сразу вслед за этим, ничтоже сумняшись, именуют их

«ключевым звеном успешного администрирования». Здорово, да! Не люди, а звенья. Но я приветствую такую откровенность. Итак, все-таки админ-фашист и здесь «рулит»!

6. Знать свое дело.

Вот это самое противоречивое место катехизиса от Red Hat Inc. Вы, наверное, подумали: составил документацию, рассказал ее наизусть, повторно инвентаризировал ресурсы, подружился с пользователями и их семьями, да еще при этом можно решить, что производил все эти действия неосознанно, без знания, что делает! Бред, конечно! Да и не о работе сисадмина здесь вообще. Вы же прочли заголовок раздела: «Изоощренная корпоративная этика». Цитирую по [6, раздел 6]: «Вы должны понимать, чем занимается ваша организация». Во как! Правда, далее они пытаются выкручиваться: «Это можно свести к одному вопросу: каково назначение систем, которые вы администрируете?». А, спрашивается, чем отличаются письма с контрактами на поставку памперсов от переписки риэлторов? Вероятно, как в известном анекдоте: пишите письма прописью – они быстрее дойдут по назначению. Завершается все репликой в стиле Дзен: «Вы обнаружите, что ваши повседневные решения стали лучше». То есть для Вас это станет полной неожиданностью. Прямо-таки корпоративная терапия!

7. Безопасность не может быть второстепенной задачей.

Начинается, как в анамнезе параноика: «Вне зависимости от того, что вы думаете о среде, в которой работают ваши системы, вы не можете считать ее безопасной. Даже автономные системы, не подключенные к Интернету, могут быть в опасности». Прочитав это, я начинаю понимать, откуда у сисадминов развивается та самая болезнь, что описала еще Эви Немет в своих трудах и заметила, что в результате ее сисадмины склонны считать все ресурсы своей собственностью [1, 32.9]. Сисадмин ни в коем случае не должен превышать свои полномочия или трактовать свои обязанности расширительно. Общечеловеческое правило «можно все, что не запрещено» в производстве не работает. Ну, ясно же, если за каждое действие заказчик должен платить, то перечень действий уже заранее описан и согласован сторонами. Но далее еще забавнее: «Это не означает, что вы должны относиться к сотрудникам как к злоумышленникам». Хм! Тогда не понятно, кто может угрожать безопасности не подключенных к Интернету систем. Наверное, «зеленые человечки»? Но потом изоощренные авторы из Red Hat Inc. начинают уже прямо противоречить своим же рекомендациям.

7.1. Риски социальной инженерии.

Здесь совершенно однозначно рекомендуется относиться ко всем пользователям как к потенциальным нарушителям. Что, в общем-то, правильно и логично. Но чуть далее все выворачивается наизнанку. Сначала странное: «На самом деле... у вас вообще не будет полномочий выработать правила, не говоря уже о том, чтобы обязывать их выполнять.» Теперь понятно, зачем надо познакомиться с пользователями поближе? Чтобы упрашивать их в приватной обстановке! Ну а потом все в точности как у Стефана Зелински в сценарии действий «идиота» в [4] ситуация 6: «Публикуйте ссылки на статьи по вопросам безопасности в вашей внутренней почтовой рассылке». Тем, кто примет эту глупость за «чистую монету», рекомендую сразу представить, как сообщение формата BagTrack получит директор его предприятия. Хотя, быть может, я не прав. Тут, скорее, предлагаются действия в стиле «технического бандита», когда упомянутый персонаж помещал советы в

практически нечитаемые источники, так как, я уверен, эти письма пользователями станут выкидываться «в корзину» без прочтения.

8. *Планировать.*

Снова, как в анекдоте: «Мужик, ты ведь не за грибами в лес ходишь?», то есть речь опять не о планировании в технологическом смысле. Это очередной гипно-блок. Его полезная нагрузка нулевая. Ну, разве можно всерьез принимать такие рекомендации, как требование экстраполировать заявления руководства: «Сказанное вскользь ... замечание о готовящемся новом проекте является верным знаком, что в скором будущем вам придется поддерживать новых пользователей». Заключение пропитано шаманизмом: «Умение видеть такие знаки (и соответствующе на них реагировать) облегчит жизнь вам...». Откровенный сюрриализм! Видать, неспроста в среде админов ходит шуточный совет «не курить» руководства, а читать.

9. *Предвидеть непредвиденное.*

Можно только продолжить императивный ряд: слышать неслышанное, догадываться о несуществующем, делать невозможное, ... пойдешь туда, не знаю куда, принеси то, не знаю что... Вероятно, последнее и является целью этой типичной нейролингвистической обработки. Как и в предыдущем разделе, сисадмину просто не дают расслабиться. Вы что-то услышали - начните об этом думать и развивать в мыслях. Если возможно предположить существование какой-то проблемы, действуйте так, будто бы она непременно случится! И вот пример: «Известно, что его (дискового пространства – А.Б.) постоянный недостаток является физическим законом, таким же, как и закон тяготения. Потому разумно предположить, что в какой-то момент вы столкнетесь с *крайней* необходимостью в дополнительном дисковом пространстве. Что же в таком случае должен делать системный администратор, который предвидит непредвиденное? Вероятно, вы можете держать несколько запасных дисков на случай аппаратных проблем». У вас еще нет нескольких дисков, лежащих в шкафу на случай непредвиденного? Немедленно пишите докладную записку руководству и потребуйте их купить! А в обоснование укажите, что «увидели непредвиденное». Но не удивляйтесь ответной реакции!

С моей точки зрения, два последних раздела «Философии системного администрирования» откровенно внушают сисадмину чувство вины за любое событие. Даже такое, что кудесниками из Red Hat Inc. приравнивается к Закону тяготения. Падают яблоки, все равно виноват сисадмин! Ну не знаю, как по версии Red Hat Inc. может спокойно спать сисадмин, обслуживающий компьютеры, которые **ОБЯЗАТЕЛЬНО** когда-то сломаются! В медицине есть соответствующий диагноз, описывающий поведение людей, навязчиво думающих о неизбежных физических явлениях. Но это тема иного исследования в изданиях для лиц другой профессии. Здесь же подчеркну, что, по сути, все разглагольствования в [6] не имеют никакого отношения к администрированию. Они, скорее, описывают правила поведения сисадмина-новичка в крупной компании: ты должен сделать все возможное и невозможное, но, что бы ты не сделал, все равно будешь неправ.

А о чем вообще речь?

Надо признать, что и Эви Немет, и Стефан Зелински гораздо ближе подошли к решению вопроса об успешной стратегии поведения сисадмина, чем сотрудники Red Hat Inc. с их незамысловатыми бойскаутскими рекомендациями. Объяснение тривиально. Этическими

нормами может обладать только личность, а не корпорация или какое-то иное юридическое лицо или государственное образование. И, значит, чем далее правила поведения личности от стереотипов поведения толпы, тем больше в них морали. Поэтому рекомендации Red Hat Inc. столь неудачны. Они вообще не служат профессиональным интересам системных администраторов, хотя и размещены в документах, предназначенных в помощь сисадминам. Остальные же просто отражают ранние фазы процесса формирования этики сисадминов.

Здесь самое время задуматься. Зачем сисадминам профессиональная этика? Есть масса профессий, которые прекрасно обходятся общечеловеческими этическими нормами. Например, сантехники не имеют собственного морального кодекса ассенизаторов. Почему, сисадмины должны обрести собственную этику?

Сначала попытаемся определить, что такое профессиональная этика. Итак, существует общечеловеческая этика. Но некоторые профессии вырабатывают собственные, отличные от всеобщих этические нормы. Такие нормы, основываясь на особенностях деятельности представителей некоторой профессии, предписывают им дополнительные ограничения. То есть, всем можно, а вот некоторым запрещено. Такие ограничения компенсируют определенные профессиональные преимущества. Например, врачебная этика запрещает врачу использовать ситуацию, создавшуюся в процессе выполнения процедуры лечения, для нанесения вреда пациенту.

Ну, скажете, да сколько угодно! Примите, какой угодно вычурный, кодекс и наслаждайтесь этой абстрактной ерундой. Но секрет не в том, чтобы самому себе выдумать правила. А в том, чтобы заставить общество признать их силу!

Вернемся к врачу. Врач, которому доверяют в силу его профессиональной этики, может оказаться объектом давления тех, кто захочет использовать данное преимущество в своих целях. И вот, общество признает за врачами право на защиту. Так, законом определяются понятия врачебной тайны. То есть врачебная этика закрепляется законодательно!

Теперь задумаемся, почему у врачей, юристов, и даже аудиторов есть признанная законом профессиональная этика, а у, например, военных ее нет! Уточню, чтобы военные и прочие служащие не обижались, и повторю: у них нет признанной законом профессиональной этики. А на все попытки ее им дать они отвечают сплоченным отказом. Например, этика служащих должна требовать публичности и прозрачности их частных бюджетов в части доходов и расходов. Они же имеют преимущество, значит, должны взять и обязательство, а не ссылаться на общегражданские права и охрану «прайвиси» тех, кто и так не имеет возможности получать взятки. А этика сотрудников правоохранительных органов, и вообще людей с оружием, должна требовать от них исключительной порядочности в его применении, а, значит, и закрепленного законом более строгого порядка наказания за злоупотребления. Но и они благоразумно предпочитают не выделяться из общей массы народа. Может быть, сисадмины тоже в числе необремененных этикой профессий?

С чего начать.

Давайте определим, есть ли в деятельности системных администраторов некоторое преимущество перед остальными гражданами, которое потребует выработки сдерживающих норм и послужит отправной точкой для создания профессиональной этики и соответствующего закона, ее защищающего.

Первое, на что можно обратить внимание, это замеченные еще Эви Немет чрезвычайные полномочия сисадминов [1, раздел 32.2] в отношении всех информационных ресурсов [3, раздел 29.2]. Припомним еще и фразочку из [1, раздел 32.14] о том, что резервная копия фактически взламывает любую защиту. Причем данное соображение имеет значимость как в отношении компаний, так и в отношении частных пользователей. Человек в своей повседневной жизни все более становится зависимым от компьютеров. Они давно стали нормой в почти каждой городской квартире. Они давно проникли в телефоны, фотоаппараты, плееры DVD и даже в стиральные машины. Все эти устройства, сопровождая деятельность человека, неизбежно накапливают информацию о тех сторонах жизни, которые принято считать личными.

Если сейчас комплекс мероприятий по изъятию информации, начинается с обесточивания мест размещения компьютеров, продолжается блокированием комнат и завершается непосредственной выемкой системных блоков, то лишь потому, что заинтересованные органы еще не догадались, что к данной процедуре можно привлечь системных администраторов, которые по закону не могут отказаться (как свидетели) и произвести выемку данных в фоновом режиме, используя служебный доступ системного администратора. Ставшие такими привычными попытки спрятать сервер вместе со всей IT-группой в подвал, в филиал, да хоть под лестницу, даже отправить сисадмина в отпуск вместе с главным бухгалтером на время проверки, пусть Вас не вводят в заблуждение: сисадмины уязвимы!

Получается, что системные администраторы рискуют подвергнуться давлению, как со стороны государства, так и со стороны работодателя. Вспомните рассуждения Эви Немет об ответственности сисадминов [3, раздел 29.3].

Это не надуманная ситуация. В подобное положение попадают все, кто в силу специфики работы проникает за границы частной жизни. Это и врачи, и адвокаты, и служители культа. Но максимальное сходство наблюдается с профессией аудиторов. Это тоже молодая профессия, и она тоже имеет дело, как с приватной, так и с производственной информацией. И вот как решается вопрос в данном случае. В Федеральном законе об аудиторской деятельности присутствует глава 8 «Аудиторская тайна» [8]. Эта глава полностью устанавливает обязанности и ответственность аудиторов перед клиентами-доверителями. Указанная норма закона служит в поддержку соответствующих принципов из Кодекса этики аудиторов России, а именно понятия о конфиденциальности и связанных с ним обязательствах [9].

Таким образом, кодекс этики системных администраторов, поддержанный законодательно, должен защитить интересы клиентов, и обеспечить гарантию прав сисадминов, в силу обстоятельств оказавшихся причастным к деловым интересам и правовым конфликтам их клиентов.

Но это лишь часть проблемы и часть возможных преимуществ. Здесь снова сделаю лирическое отступление. В нашей стране государственные мужи издавна озабочены падением престижа правоохранительных органов. А проблема решается просто! Надо выработать этический кодекс соответствующих служб и закрепить его законодательно. Что случается при нарушении этики врачом или адвокатом в культурной стране? Провинившийся не только несет ответственность в рамках закона, но и изгоняется из самой профессиональной среды. А у нас - нет! Таким путем формируется не только

уважительное отношение к профессиональной этике, но и к самим представителям данных профессий, чего у нас также не наблюдается. Какую еще выгоду получают в этом случае профессии, обладающие подобным строгим кодексом поведения? Они гарантируются от случайных стихийных конкурентов и становятся участниками культурного рынка. Ибо в противном случае лишь недогадливость клиентов, которые по замечанию наблюдательной Эви Немет [1, раздел 32.8] совершенно не понимают, какую власть над ними может иметь человек, обладающей доступом ко всем информационным ресурсам их предприятий, предохраняет сисадминов от проблем!

В заключение приведу пример из собственной практики. Один мой уважаемый заказчик, не желая держать электронные сообщения на общем сервере, забирает их не по протоколу IMAP, а по протоколу POP3. При этом ВСЕ сообщения, проходящие через почтовый сервер, ВСЕГДА дублируются в специальный пул перед фильтрацией на вирусы и спам. И, хотя я в договор обслуживания неизменно вношу пункт, обязывающий меня исключить работу на возможных конкурентов, но все-таки снимает беспокойство только вера в правоту утверждения Эви Немет на счет неисправимой неграмотности заказчиков!

Ссылки на упомянутые источники и документы:

1. Evi Nemeth, Garth Snyder, Scott Seebass, Trent R. Hein. UNIX System Administration Handbook. Prentice Hall PTR, 1995. Перевод на русский: «UNIX: руководство системного администратора», BHV, 1997.

2. Книги Эви Немет на сайте Ozon.ru.
<http://www.ozon.ru/context/detail/id/336421/>

3. Evi Nemeth, Garth Snyder, Trent R. Hein. Linux Administration Handbook. Prentice Hall PTR, 2002. Перевод на русский: «Руководство администратора Linux», Издательский дом «Вильямс», 2003.

4. Stephan Zielinski. KNOW YOUR UNIX SYSTEM ADMINISTRATOR-- A FIELD GUIDE. 1992.
<http://stephan-zielinski.com/static/sysad.txt>

5. «Об администрировании UNIX.»
http://www.sensi.org/~alec/unix/d_admin.html

6. «Философия системного администрирования» от Red Hat, Inc. в переводе И.Песина.
<http://old.linux.kiev.ua:8080/~ipesin/translations/rh-phy/ch-philosophy.html> , оригинал

7. Red Hat Enterprise Linux 3: Introduction to System Administration. Chapter 1. The Philosophy of System Administration.
<http://www.redhat.com/docs/manuals/enterprise/RHEL-3-Manual/admin-guide/ch-philosophy.html>

8. ФЕДЕРАЛЬНЫЙ ЗАКОН ОТ 7 АВГУСТА 2001 Г. N 119-ФЗ ОБ АУДИТОРСКОЙ ДЕЯТЕЛЬНОСТИ. Статья 8. Аудиторская тайна
<http://www.ckat.ru/normdoc/zau/zaus8.htm>

9. КОДЕКС ЭТИКИ АУДИТОРОВ РОССИИ. IV. ФУНДАМЕНТАЛЬНЫЕ ПРИНЦИПЫ.
16.5. Конфиденциальность.

<http://www.docaudit.ru/documents/kodeks/4/>