bhv

АЛЕКСАНДР КЕНИН

Практическое руководство системного администратора

2-е издание

- Задачи системного администратора
- Эксплуатация сети передачи данных
- Решения на основе технологий Windows и Linux
- Рекомендации по установке, настройке и оптимизации основных служб
- Секреты оптимальной и безопасной работы в Интернете
- Обеспечение работы мобильных пользователей
- Защита информации и отказоустойчивость
- Мониторинг информационных систем

СИСАДМИН
СИСТЕМНЫЙ АДМИНИСТРАТОР

Александр Кенин

Практическое руководство системного администратора

2-е издание

Санкт-Петербург
«БХВ-Петербург»
2013

УДК 004
ББК 32.973.26-018.2
К33

Кенин А. М.

К33 Практическое руководство системного администратора. — 2-е изд., перераб. и доп. — СПб.: БХВ-Петербург, 2013. — 544 с.: ил. — (Системный администратор)

ISBN 978-5-9775-0874-2

Практическое руководство к действию для системных администраторов, создающих и эксплуатирующих информационные системы офиса. Параллельно рассмотрены решения на основе технологий Windows и Linux. Приведены рекомендации по установке, настройке и оптимизации основных служб информационной системы, организации работы системного администратора, развертыванию операционных систем Windows и Linux (Ubuntu), программ корпоративной работы, мониторинга состояния серверов. Особое внимание уделено вопросам обеспечения безопасности и надежности. Даны конкретные советы по настройке основных сетевых служб, обеспечению распределенной работы в Интернете. Описана технология разрешения проблем в работе операционной системы и прикладных программ и их совместная тонкая настройка.

Второе издание доработано с учетом выхода новых версий ПО и появления новых технологий.

Для системных администраторов

УДК 004
ББК 32.973.26-018.2

Группа подготовки издания:

Главный редактор	*Екатерина Кондукова*
Зам. главного редактора	*Евгений Рыбаков*
Зав. редакцией	*Екатерина Капалыгина*
Редактор	*Анна Кузьмина*
Компьютерная верстка	*Ольги Сергиенко*
Корректор	*Зинаида Дмитриева*
Дизайн серии	*Инны Тачиной*
Оформление обложки	*Марины Дамбиевой*

Подписано в печать 30.04.13.
Формат 70×100$^{1}/_{16}$. Печать офсетная. Усл. печ. л. 43,86.
Тираж 1500 экз. Заказ №
"БХВ-Петербург", 191036, Санкт-Петербург, Гончарная ул., 20.

Первая Академическая типография "Наука"
199034, Санкт-Петербург, 9 линия, 12/28

ISBN 978-5-9775-0874-2

Оглавление

Предисловие

Эта книга написана для всех тех, кто занимается эксплуатацией и развитием информационных систем. Вы держите в руках уже второе издание, которое существенно доработано и дополнено по отношению к предыдущим выпускам.

В каждой информационной системе есть компоненты, работа которых обеспечивает стабильность всех приложений. Администратору важно правильно настроить и сопровождать функционирование базовых служб. В этой книге мы рассмотрим вопросы, связанные с установкой, настройкой и обслуживанием системы передачи данных, базовых сетевых сервисов (DHCP, DNS и др.), систем обеспечения совместной работы пользователей (электронная почта, порталы) и контроля состояния информационной системы. Все то, с чем каждодневно приходится сталкиваться администратору. Учитывая, что современные информационные системы интегрируют как Windows-, так и Linux-компьютеры, я постарался привести параллельные рекомендации.

В силу ограниченности ресурсов сопровождением информационных систем в малых и средних организациях часто занимаются специалисты, вынужденные одновременно работать в нескольких структурах. Часто им просто не хватает времени, чтобы изучить функции того или иного продукта, иногда внедрение и поддержка нового функционала просто расценивается как излишняя, неоплачиваемая нагрузка. Поэтому я постарался показать, как те или иные возможности современного программного обеспечения позволяют обеспечить более комфортную работу.

Настоящая книга предназначена в помощь тем системным администраторам, которые хотят наиболее эффективно задействовать возможности современных технологий. В ней я постарался изложить практические рекомендации по администрированию информационных систем, уделяя основное внимание конкретным советам по настройке применяемых продуктов.

В информационных технологиях очень важен показатель удовлетворенности клиента. Также и автору хотелось бы получить ваши отзывы, замечания, предложения, которые могли бы улучшить эту книгу, сделать ее более полезной на практике. Их можно отправить на адрес издательства или мне по электронной почте на **kenin@hotbox.ru**.

Ваш Александр Кенин

ГЛАВА 1

Системный администратор

Не подлежит сомнению, что ведущая роль в управлении информационной системой принадлежит системным администраторам. При том, что в нашей стране часто не формализованы требования к этой профессии.

Квалификационные требования к системным администраторам

Каждая организация имеет свою уникальную информационную систему и предъявляет к соискателям на должность системного администратора различные требования. Тем не менее можно выделить некоторые типовые параметры.

Во-первых, информационные системы бывают различной сложности. Принято классифицировать их по размеру — по числу компьютеров. В малых организациях число компьютеров составляет не более 10—15 единиц, в больших — более сотни. Понятно, что уровень требований к системному администратору будет разным в случае большой или средней организации.

> ***Примечание***
>
> Критерии размеров организаций различны для реалий нашей страны и западных компаний. Обычно размер компании в нашей стране, определяемый по числу компьютерных систем, соответствует меньшему уровню западной фирмы. Это следует учитывать, например, оценивая рекомендации по выбору программного обеспечения и т. п.

Во-вторых, по степени подготовленности можно выделить несколько уровней системных администраторов.

Начинающий системный администратор

Обычно от такого специалиста требуется точное выполнение указаний руководителя (опытного администратора). Большей частью начинающему системному администратору поручается взаимодействие с конечными пользователями.

Поэтому требования к нему могут быть сформулированы так:

- умение взаимодействовать с пользователями;
- углубленное знание операционной системы рабочей станции (настройка прав пользователя, знание особенностей структуры домашних папок, умение вылечить систему от последствий вирусной атаки и аналогичные компетенции).

"Младший" системный администратор

Будем называть такого специалиста *младшим* администратором только для того, чтобы отличать его от начинающего системного администратора. В принципе, этот уровень соответствует начальной степени подготовки администратора, которую он может приобрести примерно за 2—3 года работы.

Такой администратор может сопровождать небольшую информационную систему либо работать в качестве помощника администратора крупной организации.

В дополнение к требованиям, изложенным для начинающего администратора, для этого уровня добавляются следующие критерии:

- понимание особенностей функционирования сетевой инфраструктуры (знание основ маршрутизации, умение добавлять станции в домен, предоставлять в пользование и подключаться к общим ресурсам, диагностировать сетевые проблемы и т. д.);
- фундаментальные знания операционной системы и практические навыки работы (обслуживание баз, разбиение дисков, создание и мониторинг логических массивов, резервное копирование и восстановление операционных систем и прикладного ПО и т. п.);
- умение составлять сценарии управления на одном из языков программирования.

Системный администратор

Этот "базовый" уровень должен соответствовать следующим требованиям:

- умение самостоятельно организовывать свой рабочий день;
- качественное сопровождение пользователей (умение общаться, решать проблемы и т. п.);
- умение проводить обучение сотрудников, готовить необходимые презентации;
- практический опыт настройки основных программных систем (почтовой системы, межсетевого экрана, параметров безопасности, различных вариантов разворачивания систем и т. п.);
- фундаментальное знание операционной системы;
- умение устранять сбои в работе системы (выявлять узкие места, производить отладку в случае необходимости, пользоваться снифферами и т. п.);
- умение составлять и отлаживать сценарии на основных языках. Умение модифицировать (приспосабливать) сценарии управления к потребностям собственной системы.

Опытный системный администратор

Администратор данного уровня должен:

- ❒ уметь общаться с сотрудниками, с представителями смежных организаций, с вендорами, уметь готовить презентации;
- ❒ быстро и полностью решать проблемы в информационной системе;
- ❒ уметь выделять задания, выполнение которых можно автоматизировать, и реализовывать соответствующие алгоритмы;
- ❒ глубоко понимать операционную систему и принципы сетевого взаимодействия;
- ❒ программировать на основных языках управления, иметь опыт составления собственных программ.

Опытный системный администратор должен уметь управлять сложной информационной системой (в том числе распределенной, с большим числом мобильных пользователей). Он должен быть способен выполнять роль технического руководителя для других системных администраторов, программистов и т. д.

Как правило, для такого специалиста требуется не менее чем 5-летний опыт работы в области системного администрирования.

Дополнительные требования

Вы не могли не заметить, что в качестве требований были указаны, в общем-то, общие характеристики, предъявляемые к должности. Понятно, что в каждой организации требования к вакансии системного администратора обычно конкретизируются по следующим позициям.

- ❒ **Знание конкретных операционных систем.** Это могут быть различные выпуски Windows, клоны Linux, операционные системы Oracle Solaris, HP AIX, Red Hat и пр., которые эксплуатируются в организации. Часто от претендентов при приеме на работу требуются только базовые навыки с последующей обязанностью досконального изучения в ходе эксплуатации.
- ❒ **Умение специального программирования.** Например, от администратора может потребоваться умение устранить ошибку (или отладить сценарий) в 1С.
- ❒ **Опыт сетевого администрирования.** Может потребоваться знание сетей Novell, умение настройки протоколов маршрутизации (OSPF, BGP и т. п.), наличие опыта работы с протоколом PPP и т. п.
- ❒ **Особые требования по информационной безопасности.** Например, настройка межсетевых экранов конкретных вендоров, умение разворачивать систему PKI, опыт настройки аутентификации по смарт-картам, знание основ шифрования данных и цифровой защиты документов и т. п.
- ❒ **Требования по умению документировать.** От администратора может потребоваться умение описывать информационную систему, составлять инструкции для пользователей и т. п.

- **Опыт работы с базами данных.** Часто от администратора требуются навыки администрирования баз данных (резервное копирование и восстановление данных, экспорт информации, управление пользователями, назначение прав, настройка параметров производительности и т. д.).
- **Знание оборудования.** Как правило, от администратора требуется знание оборудования (опыт работы с ним), которое эксплуатируется в конкретной организации (например, конкретной линейки серверов, источников аварийного питания, модемов, маршрутизаторов и т. д.).

Сертификация системных администраторов

Подтверждением профессионализма администратора являются *сертификаты*, которые он может получить от тех или иных организаций. Для получения сертификата обычно требуется сдача некоторого числа экзаменов и наличие опыта работы по данному направлению. Хотя формально опыт работы и не проверяется, но, не имея его, сдать экзамен достаточно сложно.

Сертификаты бывают различными. Имеются сертификаты от вендоров (Sun/Oracle, Red Hat, Microsoft, Hewlett-Packard и др.), от организаций (например, от сообщества системных администраторов — SAGE) и др.

Традиционно наличие сертификата рассматривается кадровыми службами как дополнительный аргумент в пользу соискателя. Хотя в последнее время — по данным анализа зарубежных организаций — большинство сертификатов начинает терять свою значимость для технических руководителей. Не в малой степени этому способствуют такие случаи, когда сертификат системного инженера одного из ведущих вендоров получают 13-летние подростки, подготовленные только к ответам на тестовые вопросы.

Планирование рабочего дня

Рабочее время администратора расходуется на три основные группы задач:

- анализ состояния информационной системы;
- реагирование на события системы и обращения пользователей;
- плановые работы (расширение сети, установка новых служб, обновление программных комплексов и т. п.).

Выделяйте время на перспективные проекты

Реализация проектов требует вдумчивости и сосредоточения. Оперативная работа отвлекает от проектов, поэтому необходимо найти способ выделить время на решение стратегических задач. Если функции системного администратора возложены на нескольких специалистов, то можно так распределить обязанности, что один администратор будет заниматься обслуживанием пользователей, а другой — работать над проектом. Потом можно поменяться функциями.

Если численность специалистов не позволяет выделить специалиста для проектов, то нужно постараться так организовать работу с обращениями, чтобы высвободить хотя бы несколько часов. Для этого можно, например, предусмотреть для системного администратора "творческое время", в течение которого его можно отвлекать только для решения критических проблем, а остальные обращения будут поставлены в очередь и т. п.

Периодически анализируйте распределение своего времени. Например, если вы заметите, что значительная часть времени расходуется на поддержание функционирующего оборудования, то не лучше ли выйти к руководству с предложением об обновлении, которое будет обосновано реальными цифрами расхода времени?

Работа с пользователями

По тому, как системный администратор общается с пользователями, во многом оценивается его работа со стороны, в том числе и руководителями предприятия. По решению проблем пользователя судят о работе администратора со стороны. Пользователь не может, например, знать, что в этот момент есть другие важные проблемы, также требующие срочного разрешения. Пользователь должен ощутить внимание со стороны администратора к своему вопросу и остаться уверенным в том, что для решения его проблемы будут "брошены все силы".

Ни в коем случае нельзя разговаривать с пользователем так, чтобы акцентировать внимание на его незнании компьютера и простейших операций. Кроме сиюминутного чувства вашего превосходства такой способ общения существенно усложнит взаимодействие и только затянет решение проблемы.

Обучение системного администратора

Основную часть информации системный администратор сегодня черпает из Интернета, на специализированных форумах, в онлайновой базе знаний. Однако не следует пренебрегать и традиционными формами обучения, которые часто проводятся как подготовка по тому или иному курсу вендора.

Такие очные формы обучения полезны тем, что дают более общий взгляд на продукт, позволяют ознакомиться со всеми функциями программного обеспечения, а не только с теми, которые используются на практике в данной организации. Кроме того, преподаватели часто рассказывают об особенностях продукта, ошибках и ограничениях, о которых не пишут в рекламных документах и не сообщают на бесплатных презентациях. На таких курсах традиционно развернуты полигоны, где можно протестировать различные возможности программного обеспечения или оборудования.

Конечно, такой курс будет и не лишним с точки наличия соответствующей строчки в резюме.

Реализация изменений в информационной системе

Информационная система не может быть застывшей. Изменения в нее вносятся как по результатам исправления ошибок, так и в процессе планового развития. Традиционно процесс изменений включает в себя:

- ❒ планирование изменений;
- ❒ тестирование (если возможно);
- ❒ их реализацию;
- ❒ работу с изменениями, сбор информации о поведении системы;
- ❒ анализ информации, поиск и устранение ошибок в случае нестабильной работы.

Планирование изменений

Идеальным случаем является ситуация, когда изменения в системе являются штатными: они планируются заранее, тестируются по возможности и только после этого внедряются.

Если изменения касаются большинства систем, то их можно охарактеризовать уже как *критические*, поскольку их реализация может существенно осложнить функционирование бизнес-процессов.

Весь процесс изменений должен тщательно протоколироваться: от составления плана до фиксации всех операций. Часто бывает, что в случае возникновения проблем в работе администраторы предпринимают различные шаги по исправлению ошибок. Если к успеху не приводят одни настройки, то осуществляют другие и т. д. Выполненные настройки по исправлению забываются, считается, что они не повлияли на работу; ищутся новые исправления. В результате через некоторое время уже невозможно определить, какие операции повлияли на результат, и не удается полностью отказаться от промежуточных настроек системы.

Поэтому надо взять за правило документировать каждый свой шаг: что сделано, почему, записать ссылки на использованные статьи базы знаний и т. п.

Другой важный совет: не менять сразу много за один раз. Лучше провести несколько операций изменения, чем совместить их все. Это может не только много раз сэкономить время администратора, но и когда-нибудь нарушить работу системы на длительный срок.

Конечно, план внедрения специфичен для каждой организации. Но можно отметить необходимость следующих позиций:

- ❒ организация тестирования изменений на полигоне (провести обновления и проверить корректность работы всей системы);
- ❒ подготовка плана отмены изменений;
- ❒ выбор времени для изменений;
- ❒ организация оповещения пользователей;
- ❒ отключение пользователей;

- ❒ осуществление обновлений;
- ❒ проверка корректности работы;
- ❒ подключение пользователей;
- ❒ проверка корректности работы;
- ❒ документирование проведенных операций, доработка шаблона плана внедрения изменений по выявленным проблемам.

Обратите внимание, что после внедрения изменений на следующий день администратор обязательно с самого утра должен быть доступен для пользователей, поскольку не исключена возможность выявления ошибок на этапе начала работы в системе. Кроме того, недоступность администратора в такой ситуации косвенно будет характеризовать его заинтересованность в успешном функционировании информационной системы.

Планирование момента изменений и продолжительности операций

Реализуемые изменения не должны помешать работе организации в случае возникновения проблем. В зависимости от критичности планируемых изменений время их внедрения может выбираться во время обеда, перед началом рабочего дня, в ночное время или выходные дни. При этом любые изменения системы должны быть исключены в периоды плановых отчетов, на время проведения (и подготовки) серьезных совещаний и т. п.

О планируемых изменениях пользователи должны быть предупреждены заблаговременно. Можно озвучить планируемые операции на совещаниях у руководителей подразделений, оповестить конечных пользователей по электронной почте и т. п. Не следует относиться к оформлению оповещений формально: например, если изменения проводятся часто, то сотрудники вряд ли будут читать сам текст письма, они обратят внимание только на его тему. Поэтому уже по ней должно быть понятно, кого коснутся изменения. А в самом тексте следует объяснять, зачем проводятся эти изменения и кого и как предупредить о возражениях (например, если у подразделения на этот период запланированы важные мероприятия).

Планируя внедрение изменений, обязательно нужно готовить планы откатов изменений. Следует учитывать, что ошибки могут быть замечены и через некоторое время. Например, если планируется внесение изменения в бухгалтерскую программу, то ошибки в формировании квартальных отчетов могут быть обнаружены в худшем случае через три месяца. И вам необходимо иметь возможность восстановить исходный вариант отчетов и внести в него все операции за эти три месяца.

Время на реализацию изменений должно быть запланировано (запрошено) с запасом и включать в себя не только время на непосредственное изменение, но и запас на откат в случае неудачи, некоторый период на анализ ситуации и т. п.

При оценке периода операции следует учесть все факторы. Например, если обновление требует перезагрузки сервера, то следует предусмотреть время для штатного закрытия программ, сохранения данных, для периода тестирования оборудования

при старте системы и т. п. Если обновление предполагается установить на все системы с последующей перезагрузкой, то должна быть учтена и последовательная очередность выключения и включения систем (сначала должны выключаться файловые серверы, в последнюю очередь — серверы аутентификации и оборудование, обеспечивающее подключение к другим сетям, включение следует выполнять в обратной последовательности). Возможны и другие ситуации, которые нужно учитывать. Например, включение системы хранения данных (СХД) с одновременной раскруткой большого количества жестких дисков приводит к большой нагрузке на источники питания. А это может вызвать просадку напряжения и, возможно, сбои в работе другого оборудования. Поэтому резонно выделить некоторый период времени на включение СХД, во время которого не включать никакого другого оборудования.

Системный администратор как продавец ИТ-технологий

Системный администратор не является лицом, распределяющим финансовые ресурсы. Обычно на предприятиях подобные решения принимаются ИТ-директорами, в подчинении у которых находятся системные администраторы. Объективно как финансовые руководители, так и ИТ-директора не разбираются в тонкостях информационной системы и часто основывают свои решения на советах тех людей, которым они доверяют, например, сына, любящего посещать компьютерные клубы, или друга, которого считают специалистом ИТ. Или, что еще хуже, с позиций поддержки фирм, в которых работают родственники и знакомые. Без реального представления проблем, которые решаются при работе информационных систем.

Системным администраторам нужно приспосабливаться к такой ситуации. Без поддержки финансовых руководителей, ИТ-директоров, без нахождения компромиссов развитие ИТ-структуры будет неоптимальным. Системные администраторы должны поддерживать руководителей, обучать их, чаще посвящать в свои проблемы. Пытаться донести проблемы до руководителя в понятных ему терминах.

Системное администрирование обычно рассматривается только с точки зрения расходования бюджета. Но в тот момент, когда руководитель начинает понимать эффективность своих решений на практике и может оценить экономический эффект от работы системного администратора, а это происходит в случае ухудшения показателей основного бизнеса из-за проблем с работой инфраструктуры, служб и т. п., работа системных администраторов уже развалена, и службу приходится воссоздавать заново.

Чтобы не доводить информационную систему до критических показателей, системному администратору надо становиться *продавцом информационных технологий*. Он должен искать аргументы для обоснования выделения средств на поддержание и развитие системы. Желательно при этом опираться на независимые цифры. Например, на стоимость внешних контрактов, на количество обращений, зафикси-

рованных службой поддержки, на планы роста числа пользователей, отраженные в бизнес-планах предприятия, и т. д. Для этого нужно знать и свою статистику (например, количество предотвращенных сетевых атак), и тенденции в мире, решения у конкурентов... Если говорить коротко, то нужно показать, что конкретное вложение средств в ИТ-структуру отвечает *интересам руководителя*.

На практике используются два варианта финансирования: централизованное (содержание группы администраторов) и финансирование за счет отдельных проектов. Каждый вариант имеет свои преимущества и недостатки, но в любом случае требуются тщательно проработанные уровни обслуживания и контроль качества (чтобы при лучшем обслуживании группе системных администраторов выделялось больше средств, а руководители бизнеса в случае дополнительного финансирования могли ожидать улучшения качества обслуживания).

Учитывать человеческие особенности

Деятельность администратора по управлению системой не должна ухудшать комфортность работы пользователей. Поверьте, что через некоторое время пользователи все равно найдут способ, как обойти введенные администратором ограничения. А поскольку такие обходные пути менее безопасны и потенциально более рискованны, то они могут привести и к более серьезным отказам. Формально нарушение в таких случаях будет сделано самими пользователями, но первопричиной его фактически явится ваша политика.

Поэтому лучше так регулировать правила и ограничения, чтобы обеспечить необходимый уровень безопасности и надежности без существенных изменений принятой практики (если, конечно, такое возможно).

Быть в курсе

Системный администратор (руководитель группы администраторов) не должен замыкаться в проблемах информационной системы. Он должен знать приоритеты бизнеса и соответствующим образом планировать свою работу, в том числе заранее вносить предложения по изменению структуры (по созданию новых рабочих мест, в части организации работы сотрудников на дому, подключения филиалов и т. п.). Должны быть налажены отношения со специалистами юридической и кадровой служб предприятия.

Следует выделять время на участие в конференциях и семинарах. Обязательно подписаться на различные специализированные рассылки. И, естественно, не забывать и о самообразовании.

И не заблуждайтесь, считая, что все знают, например, о ваших планах модернизации информационной системы. Или о планируемых настройках. Чаще рассказывайте людям о своих намерениях, пытайтесь сделать пользователей своими сторонниками. Ну а если не можете перебороть себя, то хотя бы публикуйте минимальный объем информации на корпоративном сайте.

Ошибки администратора

От ошибок никто не застрахован. Не нужно скрывать их, как и не стоит наказывать подчиненных администраторов за неверные действия. Жестко придерживайтесь только одного правила: о возникновении проблемы должны быть оперативно проинформированы заинтересованные лица.

Чаще советуйтесь. Мнение собеседника, даже если он не является специалистом по данной проблеме, может подтолкнуть вас к решению совершенно с неожиданной стороны.

Старайтесь фиксировать все свои действия по настройке системы и соответствующие указания начальников. Если сомневаетесь в чем-то (например, в каком-то указании начальника), попытайтесь получить письменное подтверждение (по электронной почте и т. п.).

Инструкции и контрольные листы

Инструкции позволяют описать последовательность выполнения операций (например, по установке операционной системы в конфигурации конкретного отдела) и добиться идентичности результатов работы для различных специалистов. Удобно, если инструкции будут снабжены контрольными листами (обычно их принято называть *check*-листами), в которых будут последовательно перечислены все необходимые шаги. После изучения инструкции даже не совсем опытному администратору для выполнения операций достаточно будет только использовать контрольные листы, чтобы не пропустить какой-либо важный шаг в настройке системы.

Кроме того, заполненный контрольный лист является хорошим вариантом отчетности о выполненной работе. Особенно использование контрольных листов важно при выполнении серьезных изменений. Сам факт наличия контрольного листа уже будет свидетельствовать о том, что к предстоящим операциям была проведена серьезная подготовка.

Полномочия системного администратора

Фиксация полномочий и обязанностей системного администратора поможет снять многие претензии и оговорить условия выполнения специальных работ.

Так, желательно зафиксировать в соответствующих документах следующие параметры:

- четко определить обязанности, например, указать, что администраторы не поддерживают чужое ПО, самостоятельно установленное пользователем;
- распределить обязанности (если поддержку системы выполняют несколько специалистов): кто отвечает за установку ПО, кто решает проблемы сети, кто поддерживает пользователей данного подразделения и т. п.;
- определить особенности поддержки мобильных пользователей, работ на выставках, организуемых предприятием, и т. п.;

- ❒ зафиксировать временные рамки: в какое время можно обращаться пользователям, кто осуществляет поддержку после окончания рабочего времени и в выходные дни;
- ❒ выделить временные диапазоны на решение проблем (понятно, что длительность решения будет зависеть от категории проблемы, серьезности сбоя). Обязательно письменно определить экстренную ситуацию, при возникновении которой администратор имеет право самостоятельно прервать работы над некритичными проблемами;
- ❒ должны быть описаны процессы действий по инциденту (какая информация и как должна быть собрана, к кому обратиться, например, для вскрытия помещения в выходной день, как и в какие сроки проблема должна быть эскалирована, если ее не удается решить собственными силами).

Если в организации внедряется новая система

Если руководство внедряет новую информационную систему, то администратор обязан не только содействовать этому процессу, но и фактически принять на себя руководство всеми проблемами интеграции нового продукта:

- ❒ оценить простоту продукта, достаточность его функциональности (при этом и не должно быть избыточности);
- ❒ оценить открытость кода: что сделано специально для организации, передан ли этот код вам, уточнить права на него, возможность доработки кода, если организация откажется от услуг поставщика (или он прекратит существование, как часто это бывает);
- ❒ оценить процессы: что надо дополнительно сделать в уже существующем процессе, как, надо ли докупать лицензии и т. д.;
- ❒ определить, как будет организована связь с поставщиком, как он будет реагировать на ошибки, на просьбы доработки (кто и как должен сообщать об ошибках, в какие сроки должны быть проведены доработки, на каких условиях и т. п.);
- ❒ установить, как будет взаимодействовать новый продукт с существующей системой аутентификации и авторизации;
- ❒ оценить, как будет загружена сеть после его внедрения;
- ❒ установить, какие службы системы будут использованы или необходимо их установить дополнительно;
- ❒ если будет работать межсетевой экран, то поддерживают ли установленные в организации версии соответствующие протоколы;
- ❒ уточнить, использует ли продукт собственные протоколы (например, свой протокол поверх HTTP) — это усложнит настройку;
- ❒ разобраться, как будут протоколироваться операции, как можно подключить журналирование системы к существующей системе мониторинга;
- ❒ понять, работает ли продукт (есть ли его версии) под теми версиями операционных систем, которые изучены и используются на предприятии;