***Глава 11***

***Политика безопасности***

Безопасность – это гораздо больше, чем межсетевые экраны, обнаружение втор-

жений и схемы аутентификации. Эти компоненты являются ключевыми

в программе безопасности, но администраторам безопасности также необходи-

мо выполнять множество других задач, требующих различных знаний. В данной

главе мы рассмотрим все аспекты безопасности и опишем основные элементы,

необходимые компании для реализации успешной программы безопасности,

а также некоторые руководящие принципы и общие требования безопасности.

Кроме того, мы кратко обсудим, как описанные здесь подходы применяются

в компаниях различного размера, и покажем некоторые возможные отличия

применяемых вами подходов к безопасности от идеального случая.

Безопасность должна быть задачей каждого. Однако важно, чтобы в компании

были сотрудники, которые специализируются на потребностях организации,

касающихся безопасности, и уделяют им основное внимание. Безопасность – это

широкая, быстро изменяющаяся область знаний, и, чтобы идти в ногу со вре-

менем, системные администраторы, отвечающие за безопасность, должны

уделять все свое внимание области безопасности. Хорошими кандидатами для

обучения в этой области и работы в группе безопасности являются старшие

системные администраторы с подходящим образом мышления.

Безопасность данных требует больше навыков общения и связей в компании,

чем любая другая область системного администрирования. Во многих компа-

ниях люди считают компьютерную безопасность препятствием для своей рабо-

ты. Для достижения успеха вы должны разрушить этот стереотип и на макси-

мально ранней стадии принимать участие во всех проектах, которые затраги-

вают электронную безопасность компании.

С течением времени использование компьютера эволюционировало от необхо-

димости непосредственного физического присутствия до возможности удален-

ного доступа из любой точки мира. В соответствии с этим развивались и средства

и методы безопасности. Как изменятся модели доступа к компьютерам и сетям

в будущем и как это изменение повлияет на безопасность? В настоящее время

наблюдается тенденция к более широкому применению шифрования и строгой

аутентификации в противоположность физической безопасности или довери-

тельным отношениям. Каждая новая модель доступа требует все больше плани-

рования, обучения, тестирования и применения прогрессивных технологий.

***11.1. Основы***

Две основные схемы политики безопасности – это безопасность периметра

и глубокая защита.

1. **Безопасность периметра** – это что-то вроде крепости с высокими стенами.

Постройте хорошую стену – и вы сможете делать внутри что угодно. Поставьте хороший межсетевой экран на входе в вашу сеть – и вам не придется

беспокоиться о том, что будет внутри. В книге Bellovin, Cheswick and Rubin

2003 данный подход рассматривается как «твердый леденец с мягкой на-

чинкой», или политика, при которой «все яйца складываются в одну кор-

зину, а затем обеспечивается защищенность этой корзины». Проблема безо-

пасности периметра в том, что «твердая оболочка» исчезает с распростране-

нием беспроводных сетей и соединением сетей организации и партнеров.

2. **Глубокая защита** предполагает размещение средств безопасности во всех

точках сети. Например, межсетевой экран защищает организацию от атак

из Интернета, антивирусная система сканирует каждое сообщение элект-

ронной почты, на каждом отдельном компьютере установлены программы

для борьбы с вредоносными программами, а при передаче данных между

компьютерами используются шифрование и аутентификациая.

Как и в случае с проектированием других компонентов инфраструктуры, про-

ектирование системы безопасности должно быть основано на простоте, возмож-

ности нормального использования и минимализме. Сложность повышает риск

появления ошибок или уязвимостей в вашей защите. Слишком сложная систе-

ма будет негибкой, неудобной в использовании и поддержке, тем самым вынуж-

дая людей всячески обходить ее ограничения, чтобы эффективно работать.

Кроме того, в эффективной архитектуре безопасности элементы обеспечения

безопасности встроены в систему, а не являются поверхностными надстройками.

Хорошая система безопасности предполагает глубокий подход с элементами

обеспечения безопасности на всех уровнях системы. Если этих элементов нет

с самого начала, их может быть очень трудно добавить и интегрировать в даль-

нейшем.

Некоторые считают, что безопасность обратно пропорциональна удобству. То

есть обеспечение большей безопасности какого-либо объекта затрудняет его

использование. Это, конечно, было справедливо для ряда продуктов по обеспе-

чению безопасности. Мы полагаем, что, когда обеспечение безопасности осу-

ществляется правильно, учитывается и простота работы пользователей. Про-

блема в том, что часто технологии требуется несколько лет, чтобы дойти до

данного уровня развития. Например, пароли являются хорошей практикой, но

установка паролей на каждое приложение становится головной болью для лю-

дей, которые в ежедневной работе используют много приложений. Однако при

повышении безопасности за счет развертывания системы единой авторизации

увеличивается и удобство в результате усиленной безопасности при практичес-

ки полном отсутствии необходимости введения пользователями паролей.

Когда система безопасности неудобна, ваши пользователи найдут способы ее

обхода. Однако при достаточном развитии технологий безопасности система

становится более безопасной и простой в применении.

**11.1.1. Задавайте правильные вопросы**

Прежде чем реализовать успешную программу безопасности, вы должны опре-

делить, что вы пытаетесь защитить, от кого, каковы риски и расходы компании.

Эти деловые решения должны быть приняты в результате серьезного обсужде-

ния с руководством компании. Задокументируйте решения, принятые в ходе

этого процесса, и рассмотрите окончательный документ с руководством. Этот

документ должен будет развиваться вместе с компанией, но его не следует из-

менять слишком сильно или часто.

**11.1.1.1. Защита информации**

Корпоративная безопасность касается защиты активов. Чаще всего информация

является активом, наиболее важным для компании. Информация, подлежащая

защите, может принадлежать к нескольким категориям. Развитая программа

безопасности определяет набор категорий и классифицирует информацию

в них.

Классификация информации определяет, какой уровень безопасности к ней

применяется. Например, информация может быть категорирована как публич-

ная, конфиденциальная и строго конфиденциальная информация компании.

Публичная информация может включать литературу по маркетингу, руководства пользователей и публикации в журналах или на конференциях. Конфи-

денциальная информация компании может включать схемы организации, те-

лефонные справочники, внутренние новости с финансовыми результатами,

направление коммерческой деятельности, статьи по продуктам в разработке,

исходный код или политики безопасности. Строго конфиденциальная инфор-

мация должна очень серьезно отслеживаться и быть доступной только тем,

кому она действительно необходима. Она может включать переговоры по кон-

трактам, информацию о сотрудниках, особо секретные подробности разработки

продукции или интеллектуальную собственность клиента.

Другой аспект защиты информации – защита от злонамеренного изменения,

умышленной или случайной утечки информации, ее кражи или уничтожения.

**11.1.1.2. Доступность обслуживания**

В большинстве случаев компании требуется защищать доступность обслужива-

ния. Если компания в ведении бизнеса полагается на доступность определенных

электронных ресурсов, то одной из задач группы безопасности будет предотвра-

щение DoS-атак против этих ресурсов. Часто компании не думают об этом, пока

не начинают предоставлять интернет-услуги, потому что сотрудники обычно не

склонны проводить такие атаки против своей собственной компании.

**11.1.1.3. Кража ресурсов**

Иногда компания хочет защититься от кражи ресурсов. Например, если про-

изводственная линия обслуживается компьютерным оборудованием практи-

чески при полной загрузке, потому что часть вычислительных циклов компью-

тера используется для других задач, компании потребуется снизить вероятность

применения вычислительных циклов этой машины злоумышленниками. То

же самое касается больничного оборудования с компьютерным управлением,

где от доступности вычислительных ресурсов при первом требовании может

зависеть жизнь человека. Сайты электронной коммерции также могут подвер-

гнуться краже ресурсов. Их системы могут быть замедлены пиратами, скры-

вающими в инфраструктуре FTP- или чат-серверы, что приводит к потере

клиентуры.

**11.1.1.4. Выводы**

Совместно с вашей руководящей группой решите, что вам нужно защищать

и от кого, сколько это будет стоить компании и каковы риски. Определите ка-

тегории информации и допустимые для них уровни защиты. Задокументируй-

те эти решения и используйте полученный документ как основу для своей

программы безопасности. С развитием компании не забывайте периодически

переоценивать решения в этом документе совместно с руководящей группой.

**11.1.2. Документируйте**

политики безопасности компании

Политики – это основа всего, что делает группа обеспечения безопасности.

Формальные политики должны создаваться в сотрудничестве с людьми из мно-

гих других отделов. В создание определенных политик должен быть вовлечен

отдел кадров, особенно при определении политик допустимого использования,

политик мониторинга и неприкосновенности частной информации, а также при

определении и реализации санкций за любые нарушения политики. Юридический отдел должен быть вовлечен в создание политик, определяющих необхо-

димость отслеживания и преследования нарушителей, а также того, как и когда

привлекать правоохранительные органы при совершении незаконных действий.

Естественно, все политики должны быть одобрены высшим руководством.

Решения, принимаемые группой обеспечения безопасности, должны поддержи-

ваться политикой, чтобы обеспечить соблюдение решений, одобренных руко-

водством, в этой очень щекотливой области. Эти политики должны быть задо-

кументированы и формально одобрены соответствующими людьми. Группу

обеспечения безопасности будут просить обосновать свои решения во многих

областях, и она должна иметь возможность принимать решения с уверенностью

в том, что они находятся в полном соответствии с интересами компании, опре-

деленными руководством компании, а не группой безопасности, инженерного

обеспечения или какой-либо другой.

В разных случаях требуются различные наборы политик, и до какой-то степени

эти наборы политик будут постоянно развиваться и обновляться с возникнове-

нием новых ситуаций. Однако для начала можно взять следующий набор общих

политик.

Политика допустимого использования (Acceptable Use Policy – AUP) опре-

деляет правомочных пользователей компьютерных и сетевых ресурсов,

а также то, для чего им разрешено использовать эти ресурсы. AUP также

может включать некоторые явные примеры недопустимого использования.

Правомочные пользователи компьютерных и сетевых ресурсов перед полу-

чением доступа к ним должны подписать экземпляр этой политики, под-

тверждая, что они прочли ее и согласились с ней. При наличии в компании

нескольких зон безопасности может применяться несколько AUP.

Политика мониторинга и неприкосновенности личной информации опи-

сывает мониторинг компьютерных и сетевых ресурсов компании, в том

числе мониторинг деятельности на отдельных компьютерах, сетевого тра-

фика, электронной почты, обзора веб-страниц, журналов регистрации со-

бытий и логов. Поскольку мониторинг может расцениваться как посяга-

тельство на личную информацию, в политике должно быть в явном виде

указано, на какой уровень неприкосновенности личной информации может

рассчитывать человек при использовании этих ресурсов, если он вообще

есть. Иногда местные законы устанавливают, что может и что не может

входить в эту политику, особенно в Европе. Опять же, каждый человек дол-

жен прочитать и подписать экземпляр этой политики, прежде чем полу-

чить доступ к ресурсам.

Политика удаленного доступа должна объяснять риски, связанные с полу-

чением доступа к сети людьми, не имеющими на это права, описывать необ-

ходимые меры предосторожности для «секретных» данных человека – па-

роля, персонального идентификационного номера (Personal Identification

Number – PIN) и т. д. – и обеспечивать способ оповещения об утерянных

или украденных данных для удаленного доступа, чтобы их использование

можно было быстро запретить. Эта политика также должна содержать не-

которые вопросы личного характера – например, о размере обуви и люби-

мом цвете, – при помощи которых люди могут быть идентифицированы по

телефону. Каждый должен заполнить и подписать копию этой политики

перед разрешением удаленного доступа.

Политика сетевых соединений описывает, как компания устанавливает се-

тевые соединения для других субъектов или некоторых общих ресурсов для

доступа третьих сторон. Каждой компании в определенный момент потре-

буется установить деловые отношения с другой компанией, что потребует

более простого доступа к сети и, может быть, наличия некоторых общих ре-

сурсов: расширенной интрасети. Вы должны заранее подготовиться к это-

му. Политика должна быть распространена по всем уровням руководства

и предусматривать участие группы обеспечения безопасности на макси-

мально ранней стадии. В политике должны быть перечислены различные

поддерживаемые типы соединений и общих ресурсов, офисы, которые мо-

гут поддерживать соединение с третьими сторонами, и типы поддерживае-

мых соединений.

Политика ведения журналов (или логов) описывает, что заносится в жур-

налы и на какой срок. Журналы полезны для отслеживания нарушений бе-

зопасности после того, как они произошли, но могут занимать большие объ-

емы дискового пространства при отсутствии временных ограничений. Так-

же важно знать, существуют ли логи определенной даты, в случае вызова

в суд по уголовному делу.

**11.1.2.1. Получите поддержку высшего руководства**

Для того чтобы быть успешной, программа безопасности должна получить под-

держку высшего руководства. Руководство компании должно быть вовлечено

в создание политик и правил в программе безопасности, чтобы принимались

правильные для бизнеса решения и чтобы руководство понимало, какие реше-

ния были приняты и почему. Если вы хотите приобрести авторитет как пред-

ставитель группы обеспечения безопасности, вам потребуется умение ясно

объяснить возможности, риски и преимущества, и это нужно будет сделать на

деловом языке, а не техническом жаргоне.

В некоторых случаях сотрудники, обеспечивающие безопасность, могут не со-

гласиться с решениями, принятыми руководством компании. Если это случит-

ся с вами, попробуйте понять, почему были приняты такие решения. Помните,

что у вас может не быть доступа к той же информации или такого знания биз-

неса, как у руководящей группы. В деловых решениях принимаются во внима-

ние как технические, так и нетехнические потребности. Если вы хороший

представитель группы обеспечения безопасности1, вы должны понимать, что

руководство принимает решения, которые считает лучшими для компании,

1 Если вы считаете себя недостаточно хорошим представителем группы безопас-

ности, попытайтесь понять, что вы не смогли донести и как лучше всего это

объяснить, а затем найдите еще одну возможность обсудить это. Но лучше сделать

все правильно с первого раза!

и соглашаться с ними. Люди, обеспечивающие безопасность, склонны строить

настолько безопасную систему, что ее невозможно будет завершить, если бизнес

не откажется от благоприятной возможности на рынке или не станет таким

безопасным, что его невозможно будет развивать. Важно найти баланс между

построением совершенной системы и поддержанием развития бизнеса.

Как только корпоративное решение по безопасности было согласовано, оно

должно быть задокументировано и одобрено руководством, а затем опублико-

вано в компании. В идеале директор по безопасности, который не входит в IT-

отдел компании, должен находиться на высоком уровне в иерархии руководства.

Этот человек должен иметь как навыки ведения бизнеса, так и опыт в области

защиты информации. Директор по безопасности должен возглавлять многофункциональную группу защиты информации с представителями из юридических,

кадровых, IT-, инженерных отделов, а также отделов службы поддержки

и продаж или любых, имеющихся в компании. Директор по безопасности отве-

чает за обеспечение своевременной разработки, одобрения и исполнения адек-

ватных политик и ведет деятельность группы обеспечения безопасности и за-

щиты информации в необходимом для компании направлении.

Если группа обеспечения безопасности не может полагаться на поддержку ру-

ководителей высокого уровня, программа безопасности неизбежно потерпит

неудачу. В группе безопасности будет большая текучка кадров, а выделенные

на безопасность деньги будут потрачены впустую. Поддержка высшего руко-

водства жизненно важна.

**11.1.2.2. Централизуйте полномочия**

Появляются вопросы. Возникают новые ситуации. Имея одно место для разре-

шения этих проблем, легче поддерживать программу безопасности единой

и эффективной. Должен быть совет по политике безопасности, или центральный

орган для решений, связанных с безопасностью: деловых решений, решений

в области создания политики, архитектуры, реализации, реакции на происшест­вия и проверки.

Невозможно реализовать стандарты безопасности и обеспечивать эффективную

реакцию на происшествия без центрального органа, который поддерживает

и проверяет безопасность. В некоторых компаниях есть центральный орган для

каждого автономного подразделения бизнеса и центральный орган более высо-

кого уровня для установления общих стандартов. В других случаях мы видели

орган безопасности корпоративного масштаба с одним отдельным подразделе-

нием вне его контроля, который принадлежал недавно приобретенной компании.

Если компания полагает, что какие-то автономные подразделения бизнеса

должны иметь контроль над созданием своей политики, архитектуры и т. д.,

компьютерные и сетевые ресурсы таких подразделений должны быть четко

отделены от ресурсов остальной компании. Взаимосвязи должны рассматри-

ваться как соединения с третьими сторонами, и каждая сторона должна приме-

нять к этим соединениям свои политики и архитектурные стандарты.

Несколькими автономными сетями в одной компании может быть очень трудно

управлять. Например, если у двух частей компании различные политики мо-

ниторинга без четкого разделения ресурсов подразделений бизнеса, то может

оказаться так, что одна группа безопасности будет непреднамеренно просмат-

ривать трафик сотрудника другого подразделения бизнеса, что будет противо-

речить его ожиданиям относительно неприкосновенности личной информации.

Это может привести к судебному делу и негативному общественному мнению,

а также отчуждению персонала.

На техническом уровне эффективность вашей безопасности равна эффектив-

ности ее самого слабого звена. Если к вашей сети открыт доступ из другой сети,

над которой у вас нет контроля, вы не знаете, какая связь является слабейшей,

и у вас нет над ней контроля. Вы также можете испытывать затруднения

в отслеживании нарушителя, воспользовавшегося такой открытой связью.

**11.1.3. Основы для технического персонала**

Как технический сотрудник группы обеспечения безопасности вы должны иметь

в виду несколько других принципов, наиболее важный из которых – обеспечение

ежедневных рабочих потребностей людей, которые будут пользоваться спроек-

тированными вами системами. У этих людей должна быть возможность выпол-

нять свою работу. Вы также должны быть в курсе того, что происходит

в области уязвимостей и атак, чтобы при появлении новой уязвимости или но-

вого способа атаки ваш сайт был адекватно защищен. Критическим элементом

инфраструктуры, который вам потребуется и за выбор которого вы будете отве-

чать, – это система аутентификации и авторизации. Мы дадим несколько советов

по выбору правильных продуктов для задач, в которых важна безопасность.

**11.1.3.1. Обеспечивайте потребности бизнеса**

При проектировании системы безопасности вы всегда должны знать потребности бизнеса и стремиться обеспечить их. Помните, что нет смысла в обеспечении

безопасности компании до уровня, на котором она не может вести свой бизнес.

Также помните, что другие люди в компании тоже не глупые. Если они не смо-

гут эффективно работать, пользуясь вашей системой безопасности, они найдут

способ взломать ее или обойти. Этот факт нельзя недооценивать: обходной путь,

который найдут люди, будет менее безопасен, чем система, которую вы созда-

ли. Таким образом, лучше использовать чуть менее безопасную систему, чем

такую, которую будут обходить.

1 Шпионская программа – это программа, которая наблюдает за действиями поль-

зователя и реагирует на них, например, вставляя платную рекламу при просмот-

ре веб-сайтов.

2 Червь – это программа, которая распространяется на большое количество ком-

пьютеров и позволяет злоумышленнику удаленно программировать компьютер

для выполнения своих задач.

Для эффективного выполнения потребностей бизнеса в плане безопасности вам

потребуется понять, что сотрудники пытаются делать, как они пытаются это

делать и как выглядит их рабочий процесс. Прежде чем вы сможете принять

верное решение, вам также потребуется найти все разумные технологические

реализации и очень подробно разобраться, как они работают. Верное решение

имеет следующие черты:

Позволяет людям эффективно работать.

Обеспечивает умеренный уровень безопасности.

Максимально просто и ясно.

Может быть реализовано в умеренные сроки.

**11.1.3.2. Стройте безопасность**

при помощи жесткой инфраструктуры

Создание эффективной программы безопасности требует жесткой компьютерной

и сетевой инфраструктуры, построенной с учетом безопасности. Эффективная

реализация безопасности требует наличия известных, стандартных конфигу-

раций, умения быстро и недорого строить и перестраивать безопасные системы,

умения быстро устанавливать новые программы и патчи, а также способности

хорошо отслеживать уровни патчей и версии. Постоянный процесс установки

и модернизации машин означает наличие возможности постоянно поднимать

планку защиты против атак.

Другой элемент инфраструктуры, необходимый для хорошей программы безопасности, – это процесс увольнения сотрудников из компании. Процесс уволь-

нения обычно включает уведомление отдела кадров, который, в свою очередь,

уведомляет другие отделы, например фонд заработной платы, хозяйственный

отдел и отдел информационных технологий. Наиболее полезным средством

в процессе увольнения является контрольный список для руководителя уходя-

щего сотрудника. Он должен напомнить руководителю попросить вернуть

ключи, карты доступа, удостоверение личности, средства аутентификации,

домашнее оборудование, телефонную карту компании, мобильный телефон,

пейджер, рацию и любое другое оборудование, которое может быть у человека.

Контрольный список также должен напоминать руководителю о необходимо­сти

связаться с IT-подразделением в приемлемые сроки. В IT-подразделении должен

быть эффективный, максимально автоматизированный процесс отключения

доступа сотруднику. Эффективное отключение доступа особенно важно при

увольнении сотрудника, который считает себя обиженным компанией.

Важно построить базовую системную и сетевую инфраструктуру, и сделать это

правильно, потому что от нее зависят другие аспекты, например безопас-

ность.

**11.1.3.3. Знайте об актуальных атаках**

Профессионал в области безопасности должен уметь справляться с распростра-

ненными типами атак и знать способы защиты систем компании от этих атак.

Это предполагает ежедневное чтение нескольких рассылок электронной почты

и информации на соответствующих веб-сайтах. Вам нужно отслеживать бюл-

летени безопасности поставщиков и сводки данных организаций, исследующих

вопросы безопасности.

Информационные рассылки по электронной почте обычно предоставляют экс-

плойты, которые вы можете протестировать на своих системах, чтобы оценить,

являются ли они уязвимыми. Эти рассылки часто информируют о новой уязви-

мости быстрее других, потому что в этом случае не нужно разрабатывать

и тестировать патч, прежде чем опубликовать новость. Профессионал в области

безопасности должен стараться максимально быстро узнавать о новых уязви-

мостях, чтобы оценить, как лучше всего защитить системы компании и как

проверять наличие атак, использующих эту уязвимость.

**11.1.3.4. Применяйте аутентификацию и авторизацию**

Один из важнейших элементов системы безопасности – это мощная система

аутентификации с уникальным идентификатором для каждого человека и без

учетных записей, используемых несколькими людьми одновременно. Совместно с системой аутентификации работает система авторизации, которая указы-

вает уровень доступа, разрешенный пользователю. Аутентификация дает чело-

веку идентификатор, а авторизация определяет, что ему разрешено делать.

Ролевая учетная запись – это учетная запись, которая предоставляет людям

права на выполнение одной или более задач, недоступных для выполнения

с правами обычной учетной записи. Типичные примеры включают роли систем-

ного администратора, администратора базы данных и администратора веб-сай-

та. Общие учетные записи, даже общие ролевые учетные записи, нужно исклю-

чить. Например, ролевая учетная запись может называться dbadmin и любой

человек, которому нужно управлять записями баз данных, способен воспользо-

ваться для этого данной учетной записью. Пароль известен всем, кому нужен

доступ. Общие учетные записи затрудняют отчетность, если не делают ее вооб-

ще невозможной. В случае возникновения проблем может оказаться, что невоз-

можно найти виновного. Также в этом случае может быть гораздо труднее

полностью отключить доступ человеку, уходящему из компании. Системные

администраторы вынуждены проверять, к каким ролевым учетным записям

человек имел доступ, и причинять неудобства другим, меняя пароли на этих

учетных записях.

В большинстве операционных систем есть другие механизмы обеспечения од-

ного уровня доступа нескольким людям, которые идентифицируются как отдельные субъекты. Проверьте возможности своей системы, прежде чем принять

решение воспользоваться общей учетной записью. Например, людей, которым

нужен доступ к учетной записи dbadmin, можно вместо этого добавить в группу

dbadmin, которая позволяет им действовать в качестве администратора базы

данных. Учетная запись root в UNIX – ролевая учетная запись, как и Администратор

в Windows. Лучше дать кому-то права PowerUser в Windows на необходимых

машинах или права Администратор домена, если человеку нужен привилегирован-

ный доступ на всех мащинах. Системы жесткой аутентификации обычно за-

трудняют создание общих учетных записей.

Система жесткой аутентификации предоставляет вам большую степень уверен-

ности, что человек, которого компьютер считает прошедшим аутентификацию,

действительно этот человек, а не просто кто-то, использующий его учетные

данные (пароль). Например, система жесткой аутентификации может быть

биометрическим механизмом, таким как сканер отпечатка пальца или глаза,

или системой, основанной на карманных устройствах, для которой человеку

нужно физическое устройство (идентификатор), а также секретные данные,

например PIN-код, который он помнит. Человек, который передает кому-то свое

физическое устройство, больше не имеет доступа, что часто является достаточ-

ным затруднением для совместного использования. Если устройство будет по-

хищено, то похититель не будет знать секретный PIN-код. Другими словами,

система карманных идентификаторов требует чего-то, что у вас есть, и чего-то,

что вы знаете.

Карманный идентификатор проще носить, если у него есть другие функции.

Другими словами, если это еще и брелок, люди будут носить его с собой, потому

что он будет полезен им не только для загрузки компьютеров. Это также при-

вязывает его к чему-то, что важно для человека лично, к дому или машине,

снижая таким образом вероятность передачи другому лицу.

Системы жесткой аутентификации обычно не являются гибкими. Но иногда

в экстренных случаях требуется небольшая гибкость. Время от времени в меха-

низме жесткой аутентификации что-то может работать неправильно и вам по-

надобится способ аутентификации людей по телефону, особенно если они путе-

шествуют. Например, кто-то может потерять или сломать физическое устройство – HHA или переносное биометрическое устройство, – необходимое для аутен-

тификации. Вам нужно подготовиться к такой возможности при первоначаль-

ной установке системы жесткой аутентификации.

При создании учетной записи дайте человеку заполнить форму, содержащую

вопросы об информации, которая может быть использована для аутентификации

по телефону. Например, человек может назвать свой размер обуви, любимый

фрукт, магазин, в котором была сделана конкретная покупка, место, где он

встречал новый 2000 год, любимый предмет в школе или что-то, что может быть

проверено в компании, например кто находится в соседнем офисе или за сосед-

ним столом. Для человека, который может таким образом обеспечить успешную

аутентификацию по телефону, должен быть доступен другой механизм, дающий

ему временный доступ к системам, пока проблема не будет решена. Например,

многие системы позволяют пользоваться обычным паролем в течение 24 ч или

достаточно долгое время до замены HHA.

**11.1.3.5. Матрица авторизации**

Аутентификация подтверждает личность. Авторизация – это то, что позволено

делать человеку. Например, обычному пользователю нужна возможность читать

его собственную электронную почту, но не почту других людей. Некоторые

люди должны иметь возможность чтения конкретной базы данных, меньшее

их число – обновлять данные, и только у нескольких администраторов должна

быть возможность изменять схему базы данных.

Использование матрицы авторизации, основанной на функциях подразделений

компании, категориях системы и классах доступа, более удобно, чем определение этой политики в текстовой форме. Матрица авторизации описывает уровень доступа данной группы людей к определенному классу машин. Такая политика должна разрабатываться совместно с руководством и представителями всех подразделений компании. После того как это будет сделано, система авторизации должна быть связана с системой аутентификации, которая

реализует политику. Набор идентификаторов и информация, записанная

в системах аутентификации и авторизации, являются одним из пространств

имен.

***Глава 12***

***Этика***

Какие политики, связанные с этикой, должны быть в компании? Какова допол-

нительная моральная ответственность системных администраторов и других

сотрудников с привилегированным техническим доступом? В данной главе

рассматриваются оба вопроса.

Этика, принципы поведения, которыми руководствуется группа людей, отли-

чается от морали. Мораль – это провозглашение того, что хорошо и правильно,

и она не входит в число вопросов, обсуждаемых в данной книге.

Вне зависимости от того, привлекает ли вас ваша организация к созданию эти-

ческих руководств для всех пользователей сети или только для системных ад-

министраторов, ознакомьтесь с этой главой. Мы хотим предоставить вам средст­ва, необходимые для выполнения этой работы.

***12.1. Основы***

Обычно в организациях есть различные политики, связанные с этикой, для

своих сотрудников и других филиалов. Этические нормы, связанные с приме-

нением сетей, делятся на две категории: нормы, применяемые ко всем поль-

зователям, и нормы, применяемые только к привилегированным пользовате-

лям, например руководителям, системным администраторам и администра-

торам баз данных. В принципе, системный администратор должен тщательно

соблюдать политики компании, а также быть примером для подражания.

У вас есть доступ к конфиденциальной информации, которую не может видеть

большинство других сотрудников, поэтому на вас лежит особая ответствен-

ность.

В последнее время появилось много американских и европейских правовых

нормативных документов, утвердивших более широкую ответственность кор-

пораций за соблюдение этических норм и правил в сфере IT. Такие документы,

как закон Сарбейнса–Оксли (Sarbanes-Oxley Act), Закон о правах семьи на об-

разование и неприкосновенность частной жизни (Family Educational Rights and

Privacy Act), Закон об отчетности и безопасности медицинского страхования

(Health Insurance Portability and Accountability Act – HIPAA) изменили образ

мыслей компаний относительно этих проблем. Профессия системного админис-

тратора была затронута напрямую.

341

12.1.1. Согласие, основанное

на полученной информации

Принцип согласия, основанного на полученной информации, изначально сфор-

мулированный специалистами по врачебной этике, справедлив в отношении

системных администраторов точно так же, как и в отношении врачей. Во вра-

чебной этике согласие, основанное на полученной информации, складывается

из двух частей. Сначала пациент должен быть полностью информирован о ва-

риантах лечения, всех возможных достоинствах и недостатках этих вариантов

и степени вероятности успеха. Информация должна быть представлена так,

чтобы человек ее понял, и у пациента должна быть возможность решиться на

лечение или отказаться от него без какого-либо принуждения – в этом заклю-

чается элемент согласия.

Такое согласие невозможно, если кто-то не информирован должным образом – не-

способен понять последствия – или не имеет возможности дать согласие, напри-

мер человек находится в коме и у него нет близких родственников. В таких

случаях общепринятым стандартом является полное соблюдение трех следую-

щих условий. Во-первых, у процедуры должна быть высокая вероятность успе-

ха. Во-вторых, должны учитываться прежде всего интересы пациента, чтобы

в случае успешного проведения операции человек скорее всего был бы благода-

рен впоследствии. В-третьих, сначала должны быть использованы все возмож-

ности получить согласие, основанное на полученной информации. Другими

словами, нарушение принципа согласия, основанного на полученной информа-

ции, является крайней мерой.

Эти принципы могут быть применены ко многим задачам системных админис-

траторов. Люди должны понимать правила, по которым они живут. Например,

в соглашении об уровне обслуживания (Service-Level Agreement – SLA) может

быть указано, что обслуживание будет осуществляться только в определенные

часы, и ваши клиенты должны их знать. Компьютерный сервер может быть

предназначен для выполнения долговременных задач, например симуляций.

Если у программы симуляции нет функции сохранения на контрольных точках,

из-за перезагрузки можно потерять дни и недели работы. Если перезагрузка

совершенно неизбежна, в SLA может быть указано, что текущие пользователи

машины будут уведомлены об этом, – согласие, основанное на полученной ин-

формации. С другой стороны, вычислительные серверы для задач с меньшими

затратами времени могут иметь SLA общего характера, в котором будет указа-

но только предупреждение за 15 мин. SLA информирует ваших клиентов о том,

как вы будете работать в различных ситуациях.

12.1.2. Профессиональный кодекс поведения

Гильдия системных администраторов (System Administrators’ Guild – SAGE)

и Лига профессиональных системных администраторов (League of Professional

System Administrators – LOPSA) разрешили нам напечатать последнюю редак-

цию Этического кодекса системных администраторов1. Мы делаем это, посколь-

1 SAGE – www.sage.org. LOPSA – http://lopsa.org.

Основы

342

ку считаем, что он является отличным словесным выражением наших мыслей

относительно того, что системные администраторы должны поддерживать очень

высокий уровень профессионализма. Этот документ является хорошей основой

для написания ваших собственных корпоративных правил поведения. Он на-

меренно не является сводом законов, обязательных для принудительного ис-

полнения, перечислением процедур, всеобъемлющим списком предполагаемых

ответных действий в различных ситуациях или перечислением санкций и на-

казаний.

Этический кодекс системного администратора

Профессионализм

Я буду соблюдать профессиональные нормы на рабочем месте и не позволю

личным чувствам или убеждениям заставлять меня относиться к людям не-

справедливо или непрофессионально.

Личная сознательность

Я буду честным в своей профессиональной деятельности и стану позитивно

воспринимать критику относительно моей компетенции и последствий мо-

их ошибок. Когда потребуется, я обращусь за помощью к другим.

Я буду по возможности избегать конфликтов интересов и убеждений. Когда

у меня попросят совет и при этом имеется конфликт интересов и убежде-

ний, я сообщу о последнем, если это уместно, и при необходимости отка-

жусь от участия.

Неприкосновенность личной информации

Я буду осуществлять доступ к личной информации в компьютерных систе-

мах, только когда это необходимо для выполнения моих технических обя-

занностей. Я буду поддерживать и защищать конфиденциальность любой

информации, к которой у меня может быть доступ, вне зависимости от спо-

соба, которым я ее узнал.

Законы и политики

Я буду изучать актуальные законы, нормы и политики, касающиеся вы-

полнения моих обязанностей, и обучать им других.

Общение

Я стану обсуждать с руководством, пользователями и коллегами компью-

терные вопросы, если это будет в наших общих интересах.

Я буду стараться выслушать и понять потребности всех сторон.

Целостность системы

Я буду стараться обеспечить необходимую целостность, надежность и до-

ступность систем, за которые отвечаю.

Я буду разрабатывать и обслуживать каждую систему так, чтобы это макси-

мально соответствовало ее назначению в организации.

•

•

•

•

•

•

•

•

•

Глава 12. Этика

343

Образование

Я буду улучшать и расширять свои технические знания и другие навыки,

связанные с работой.

Я буду делиться своими знаниями и опытом с другими.

Ответственность перед компьютерным сообществом

Я буду сотрудничать с более крупным компьютерным сообществом, чтобы

поддерживать целостность сетевых и компьютерных ресурсов.

Социальная ответственность

Как информированный профессионал я буду способствовать написанию

и принятию актуальных политик и правил, согласующихся с перечисляе-

мыми здесь этическими принципами.

Нравственная ответственность

Я постараюсь создать и поддерживать спокойную, здоровую и продуктив-

ную рабочую обстановку.

Я приложу все усилия для того, чтобы мои решения согласовывались с бе-

зопасностью, неприкосновенностью личной информации и благополучием

моего сообщества и общества в целом, и буду оперативно выявлять факто-

ры, которые могут представлять собой неизвестные риски или опасности.

Я буду принимать честную критику моей технической работы и честно кри-

тиковать других, а также должным образом сообщать о заслугах других

людей.

Я буду следовать примеру, поддерживая высокие нравственный стандарт

и степень профессионализма в выполнении всех своих обязанностей. Я буду

поощрять коллег и сослуживцев следовать этому этическому кодексу.

12.1.3. Руководства пользователя

В каждой организации должен быть набор руководств по допустимому исполь-

зованию компьютеров организации1. Эти руководства могут касаться некоторых

из следующих вопросов. При каких обстоятельствах допускается использование

оборудования работодателя в личных целях? Какие типы использования

в личных целях запрещены? Может ли сотрудник посещать обычный интернет-

магазин со своего рабочего места? Может ли сотрудник писать в свой блог

с работы? Как насчет использования рабочего компьютера для просмотра веб-

сайтов «для взрослых»? Как меняются правила, если сотрудник пользуется

оборудованием компании дома?

•

•

•

•

•

•

•

•

1 Интернет-провайдеры часто называют эти соглашения политикой допустимого

использования (Acceptable Use Policy – AUP); в учебных заведениях они нередко

называются правилами поведения пользователей (User Code of Conduct – UCC).

Эти термины взаимозаменяемы.

Основы

344

Правила поведения должны определять и запрещать опасные или мешающие

связи, объяснять, как сообщать о них и как обрабатываются эти сообщения.

Иногда эти указания являются частью политики допустимого использования,

рассмотренной в главе 11.

Правила поведения в учебных заведениях обычно сильно отличаются от таковых

в бизнесе. Различия связаны с требованиями свободы обучения и тем, что для

многих студентов университетский комплекс является домом.

Образцы политик можно найти через различные деловые и учебные ассоциации,

у которых часто есть веб-сайты с набором политик различных организаций.

Одним из таких архивов является Dijker 1999. Лучший способ написать поли-

тику – это найти архив и политику, философия которой наиболее близка к ва-

шей, и использовать ее в качестве базового документа.

12.1.4. Правила поведения

привилегированных пользователей

Некоторым пользователям для выполнения работы нужен привилегированный

доступ. Возможности писать и отлаживать драйверы устройств, устанавливать

программы для других людей и выполнять многие другие задачи требуют до-

ступа с правами root, или правами Администратора. Организациям требуются

специальные правила поведения для этих людей, потому что, как мы все знаем,

привилегиями могут злоупотреблять. Эти нормы поведения должны включать

следующие пункты.

Человек признает, что привилегированный доступ предполагает ответственность за его надлежащее использование.

Человек обещает использовать высокие привилегии доступа исключитель-

но по служебной необходимости. Руководство должно в явном виде опи-

сать, что является таким использованием.

Компания признает, что люди могут совершать ошибки, и обеспечивает

процедуры минимизации ущерба, к которому может привести ошибка. На-

пример, системные администраторы должны делать резервные копии пе-

ред любыми изменениями.

Должны быть определены процедуры, предписывающие, что делать, если

благодаря привилегированному доступу кто-то получает информацию, ко-

торая иначе не стала бы известной. Например, предположим, что систем-

ный администратор устраняет проблему на почтовом сервере и случайно

видит сообщение, показывающее, что кто-то играет на рабочем месте в сете-

вые азартные игры. Как должен поступить системный администратор? По-

литика должна описывать, каких действий организация ждет от системно-

го администратора.

Рассмотрим другой пример. Допустим, привилегированный пользователь

узнает о чем-то не преступном, но также важном, например, об ожидаемом

слиянии. Как должен поступить системный администратор. Опять же, нор-

мы поведения должны быть явными и должны указывать, что необходимо

делать сотруднику, узнавшему важную информацию компании.

Последствия ошибки должны быть указаны. Мы полагаем, что в данном

случае лучшая политика – отсутствие наказания за ненамеренную ошибку,

если о ней было своевременно и честно сообщено. Чем раньше будет сообще-

•

•

•

•

•

Глава 12. Этика

345

но об ошибке, тем быстрее она может быть исправлена и тем меньший ущерб

она вызовет из-за цепной реакции.

Нужно предупредить о возможных санкциях за нарушение политики,

вплоть до увольнения.

Сотрудники с привилегированным доступом должны дать расписку в том, что

они прочитали нормы поведения для привилегированных пользователей. Ори-

гинал этой расписки должен храниться у руководителя сотрудника или в отде-

ле кадров, в зависимости от существующего в организации порядка. Как со-

трудник, так и его руководитель должны получить копию расписки.

В качестве эффективной меры безопасности группа системных администраторов

должна отслеживать, у кого есть привилегированный доступ к каким системам.

Подобная практика особенно полезна, когда нужно сообщать системным адми-

нистраторам о необходимости отключить привилегии доступа, в случае если

привилегированный пользователь покидает организацию. В некоторых орга-

низациях есть политика, согласно которой срок действия привилегированного

доступа заканчивается через 12 месяцев, если соответствующий документ не

будет подписан повторно. Эта практика предполагает регулярный пересмотр

политики. Еще одним хорошим средством являются автоматические напоми-

нания.

Том дает младшим системным администраторам, которых он нанимает, следу-

ющие инструкции:

Три правила привилегированного доступа Тома

(1) Будьте внимательны. (2) Уважайте неприкосновенность личной ин-

формации. (3) Если вы что-то испортите, сразу говорите мне.

Правило 1: Будьте внимательны.

Вы можете нанести большой ущерб, являясь пользователем root/Адми-

нистратор, администратором базы данных и т. д., поэтому будьте внима-

тельны. Делайте резервные копии. Сделайте паузу, прежде чем нажать

клавишу Enter. Делайте резервные копии. Проверяйте групповые симво-

лы, прежде чем их применять. Делайте резервные копии. Внимательно

относитесь к тому, что вы выполняете. Делайте резервные копии. Не

пейте во время работы с компьютерами. Делайте резервные копии.

Правило 2: Уважайте неприкосновенность личной информации.

Не смотрите на то, что не требуется для выполнения задачи. Не «просмат-

ривайте». Не смотрите чьи-то данные, если вы не хотите, чтобы кто-то

просматривал ваши аналогичные данные.

Правило 3: Если вы что-то испортите, сразу говорите мне.

Вы будете делать ошибки. Это нормально. Вы никогда не будете наказа-

ны за честную ошибку, если скажете мне о ней, как только поймете, что

не можете ее исправить. Скорее всего, исправление ваших ошибок входит

в мои обязанности, и вы должны будете смотреть, как я это делаю. Чем

быстрее вы мне сообщите, тем лучше будет мне, потому что мне придется

меньше исправлять. Однако, если вы скроете ошибку и мне придется

исправлять ее, не зная, что она была сделана, я узнаю, какая была ошиб-

ка, кто ее сделал, и у вас будут неприятности.

•

Основы

346

Нужное напоминание в нужное время

Популярная программа sudo (Snyder et al. 1986) предоставляет ограни-

ченный привилегированный доступ к UNIX-системам. Определенные

версии sudo выводят сообщение:

«Мы надеемся, что вы получили стандартные указания от вашего сис-

темного администратора. Обычно они сводятся к следующему:

1. Уважайте неприкосновенность личной информации других людей.

2. Думайте, прежде чем печатать.»

Эта программа прекрасно и своевременно напоминает людям о политике.

Имейте свидетелей

Нестабильно работающий почтовый сервер компании повреждал почто-

вые ящики сотрудников. Пока патч для программы не вышел, системные

администраторы обнаружили, что почтовые ящики можно было испра-

вить при помощи текстового редактора. Однако во время исправления

почтового ящика системные администраторы могли видеть сообщения

сотрудников. Когда был поврежден почтовый ящик генерального дирек-

тора, системные администраторы столкнулись с проблемой. В отрасли

происходило много слияний, и системные администраторы не хотели

брать на себя ответственность, связанную со случайным ознакомлением

с важным сообщением из почтового ящика генерального директора. Они

решили, что за работой по исправлению почтового ящика генерального

директора будет наблюдать его помощник. Таким образом, помощник

видел, что системный администратор не разглядывал конфиденциальную

информацию, и знал, какая часть конфиденциальной электронной почты

генерального директора была просмотрена. Это защищало как генераль-

ного директора, так и системного администратора.

Иногда эти политики регулируются федеральным законодательством. Напри-

мер, Комиссия по ценным бумагам США (Securities and Exchange Comission –

SEC) определила правила, запрещающие мониторинг сетей, используемых на

фондовом рынке, что может сильно затруднить устранение сетевых неполадок

на Уолл-стрит. Федеральная комиссия связи США (Federal Communications

Commission – FCC) также имеет правила, регулирующие, как телефонные опе-

раторы и технический персонал могут использовать информацию, случайно

полученную во время работы. Эти люди могут обсуждать данную информацию

только с ее источником и не могут использовать ее для личной выгоды.

Наконец, сами пользователи сети должны понять, что мониторинг может быть

элементом обслуживания сети. Должна быть политика мониторинга и непри-

косновенности личной информации, рассмотренная в разделе 11.1.2.

Глава 12. Этика

347

12.1.5. Соблюдение авторских прав

В организациях должны быть политики, в которых указано, что сотрудники

обязаны соблюдать законы об авторском праве. Например, компьютерное пи-

ратство распространено повсеместно и многие люди не понимают, что «одол-

жить» программу, не предназначенную для свободного распространения, на

самом деле значит украсть ее1.

Компании очень заботятся о том, чтобы не быть уличенными в использовании

пиратского программного обеспечения. Финансовые обязательства и негативное

общественное мнение не очень приятны для руководителей и акционеров. До-

бавьте к этому рейды, открыто проводимые организациями по борьбе с компью-

терным пиратством, и получите рецепт катастрофы. Вывод: не используйте

пиратских программ на оборудовании компании и не позволяйте пользователям

делать это тайком.

Советовать людям не пользоваться пиратскими программами не особенно эф-

фективно, они всегда убеждены, что то, что они делают, не является компью-

терным пиратством. Многие не понимают, что является пиратством, а если

и понимают, то будут ссылаться на незнание, когда их поймают. «Я думал,

у нас была корпоративная лицензия». «Я не знал, что она была установлена на

еще одной машине». «Мне кто-то сказал, что все нормально».

Чтобы решить эту проблему, политика соблюдения авторских прав должна

представить 3–4 примера наиболее распространенных нарушений. Например,

в ней можно указать, что компьютерные программы с индивидуальной лицен-

зией должны приобретаться для отдельных компьютеров и что установочный

диск не должен использоваться на нескольких машинах. Также политика может

требовать, чтобы руководства и материалы для программного обеспечения хра-

нились в одной комнате с компьютером, на котором оно установлено.

Некоторые компании наказывают сотрудников за установку любых программ

без явного одобрения руководства. В качестве альтернативы и ради простоты

в политике могут быть указаны программы, которые сотрудники могут свобод-

но загружать, например новые версии Adobe Acrobat Reader или веб-броузеров.

Установка программ, которые не входят в список, должна быть одобрена руко-

водством.

Наконец, полезным может быть пункт приблизительно следующего содержания:

«Мы все стараемся снизить лишние расходы, и мы ценим ваши усилия в этой

области. При этом пиратское программное обеспечение является средством

снижения расходов, но мы не признаем его легитимной мерой. Никому в этой

компании не разрешается заниматься пиратством, если кто-либо будет устанав-

1 Пиратское программное обеспечение также представляет собой средство распро-

странения компьютерных вирусов и поэтому является проблемой безопасности.

В наши дни вирусы, распространяемые с пиратскими программами, редко заме-

чают, потому что обычно они переносятся по Интернету с помощью электронной

почты. Однако справедливости ради следует заметить, что была пара случаев,

получивших широкую огласку, когда вирусы распространялись посредством

коммерческих, упакованных в архив программ.

Основы

348

ливать пиратское ПО или попросит об этом вас, пожалуйста, выполните эту

процедуру».

Самый простой способ обеспечить соблюдение политики – это пойти путем на-

именьшего сопротивления: покупайте популярные программы с лицензиями

на все рабочие станции. Вы не сможете нарушить правила, если у вас есть кор-

поративная лицензия. Устанавливайте их в стандартном комплекте програм-

много обеспечения на все рабочие станции. Люди вряд ли будут искать альтер-

нативные программы, если они без проблем могут использовать программы, на

которые у вас есть лицензия. Если это нереально, в качестве другого подхода

можно требовать, чтобы все заявки на покупку новых рабочих станций или

серверов включали также необходимые операционные системы и приложения

или лицензии на них.

Одним из главных преимуществ бесплатного и открытого программного обес-

печения является то, что лицензии разрешают копирование, если не активно

призывают к нему. Лицензия, которую надо соблюдать, все же существует, но

обычное использование редко вызывает проблемы. Если сотрудники изменяют

исходный код или используют исходный код в качестве элемента другого про-

дукта, нужно внимательно изучить лицензию. В некоторых крупных компани-

ях есть выделенная группа для глобального управления соблюдением лицензий

по бесплатному/открытому программному обеспечению и поиска путей более

эффективного использования их вовлеченности в сообщество программного

обеспечения с открытым исходным кодом.

Важно довести до людей правду жизни: при предъявлении иска о нарушении

авторских прав компании редко признают свою вину. Вместо этого они привле-

кают к ответственности человека, который допустил это нарушение, и обвиня-

ют в нанесении ущерба его. Укажите это в своей политике и убедитесь, что эта

политика до всех доведена.

Для системных администраторов особенно важно это понять. С гораздо большей

вероятностью обвиняемым будет несчастный системный администратор, кото-

рый использовал лицензию разработчика на операционную систему для ввода

в строй новых рабочих станций, нежели менеджер, отказавшийся вовремя

подписать заказ на покупку новых лицензий. Если ваше руководство требует

от вас выполнения противозаконных действий, вежливо откажитесь, в пись-

менной форме или по электронной почте.

Простое управление лицензиями на бумаге

Администрирование массовых лицензий необязательно должно быть

сложным. Однажды Том заказал 50 лицензий на право использования

программы и одну копию документации и самой программы. Затем он

пронумеровал 50 строк на листе бумаги и, когда кому-то требовалась

программа, вписывал в строку имя этого человека. Этот лист он вложил

в руководство по установке. Это решение очень эффективно работало

и требовало минимальных усилий – не нужно было поддерживать базу

данных и не было дополнительных расходов.

Глава 12. Этика

349

Простое отслеживание лицензий при помощи групп

Есть очень простой способ отслеживать лицензии на программное обес-

печение по сети. Допустим, у вас есть лицензия на 50 копий программы,

которые можно выдавать людям, когда это потребуется. Создайте

в Microsoft ActiveDirectory или LDAP группу, названную по названию

программы (может быть, в формате lic\_Название\_программы). Когда вы ус-

тановите программу на компьютере сотрудника, внесите его в группу.

Теперь вы можете сосчитать количество людей в группе, чтобы опреде-

лить, сколько было выдано лицензий. Особенно приятен тот факт, что

при увольнении сотрудника и удалении его учетной записи он будет уда-

лен из группы и лицензия освободится.

12.1.6. Работа с правоохранительными органами

В организациях должна быть политика по работе с правоохранительными ор-

ганами, чтобы системные администраторы знали, что делать, если с ними свя-

жутся их сотрудники. Сотрудники правоохранительных органов иногда обра-

щаются к системным администраторам и привлекают их для помощи в рассле-

дованиях преступлений, связанных с компьютерами, а также в делах, связанных

с сексуальными домогательствами, или других случаях, где необходимы дока-

зательства. В таких ситуациях естественной реакцией может быть паника,

поэтому, а также для того, чтобы избежать нарушения закона или политики

компании, системным администраторам нужна соответствующая процедура.

Вообще говоря, хорошая идея – работать с правоохранительными органами

через руководителя. В одной компании была следующая процедура:

Если с вами связались правоохранительные органы

1. Расслабьтесь. Будьте спокойны.

2. Будьте вежливы (у системных администраторов часто бывают про-

блемы с отношением к власти, и им нужно напоминать, что грубить

следователю – плохо).

3. Передайте дело своему руководителю. Можно сказать следующее:

«В соответствии с нашей политикой мы охотно сотрудничаем с право-

охранительными органами. Я должен сказать об этом своему началь-

нику. Не могли бы вы оставить свой телефон, чтобы он вам позвонил?»

(Сотрудники правоохранительных органов всегда дадут свой номер

телефона. Шутники и аферисты – нет.)

4. Если вы руководитель, свяжитесь с юридическим отделом для консуль-

тации.

5. Записывайте все требования, все телефонные звонки, связанные с об-

суждением этих требований, и все введенные команды.

Основы

350

6. Системный администратор, собирающий доказательства, должен пе-

редавать их в юридический отдел, который, в свою очередь, предоставит

их правоохранительным органам, если руководитель не даст других

указаний. (Такаяполитика защищает системного администратора.)

7. Если с вами связалась внутренняя корпоративная служба безопасности,

доказательства необходимо передать руководителю, который должен

предоставить их сотрудникам службы безопасности. Будьте вежливы,

разъясняя эту политику корпоративной службе безопасности: «Мы всег-

да выполняем требования вашего отдела. Однако политика нашего отдела

предписывает мне собрать эти материалы и передать их моему начальни-

ку, а затем он передаст их вам. Связаться с моим начальником можно…»

Организация обязана проверять личность человека, который говорит о себе как

о сотруднике правоохранительных органов, прежде чем сообщать ему что-либо

вообще, в том числе имя и контактную информацию вашего руководителя.

Проводите эту проверку даже до того, как подтвердите, что вы системный ад-

министратор. Лучший способ – сказать человеку, что вам требуется проверить

его личность. Спросите номер телефона человека и номер коммутатора службы,

затем позвоните на номер коммутатора и попросите этого человека к телефону.

Если вы сомневаетесь в том, что номер коммутатора соответствует действитель-

ному, проверьте его по телефонному справочнику.

Если вы не проверите личность человека, утверждающего, что он сотрудник

правоохранительных органов, это может привести к катастрофе. К несчастью,

некоторые злоумышленники выдают себя за сотрудников правоохранительных

органов, когда воруют информацию компании, применяя тактику, называемую

социальной инженерией. Она работает следующим образом.

1. Для начала собрать небольшое количество информации.

2. Позвонить, представившись сотрудником правоохранительных органов

или новым работником компании.

3. Использовать небольшое количество информации для получения более по-

лезной информации. Повторить то же самое с новой информацией.

4. Повторять предыдущие шаги, пока информации не будет достаточно для

нанесения серьезного ущерба.

Неудавшаяся попытка социальной инженерии

Однажды молодому, наивному системному администратору позвонил

некто и представился сотрудником местной полиции. Человек заявил,

что он проверяет, как местные компании обеспечивают безопасность

своих компьютерных сетей, в рамках программы помощи сообществу.

Он задал несколько конкретных вопросов, на которые системный адми-

нистратор охотно ответил.

В течение следующих нескольких дней некоторым сотрудникам компании

звонил тот же человек, на этот раз представляясь новым сотрудником их

группы компьютерной безопасности. Конечно, создавалось впечатление,

что он разбирается в системе. К счастью, одна женщина попыталась про-

верить его личность, и, когда это ей не удалось, она связалась с руководи-

Глава 12. Этика

351

телем группы системных администраторов. В результате руководитель

предупредил всех сотрудников компании, что действует мошенник и ник-

то не должен раскрывать важную информацию по телефону, а о любых

необычных запросах на важную информацию нужно сообщать руководи-

телю. Эти действия остановили деятельность мошенника.

Если бы злоумышленник продолжил свои поиски, он мог бы воспользовать-

ся своими методами для получения доступа к корпоративной сети. Напри-

мер, когда он выдавал себя за сотрудника группы обеспечения безопасности, это казалось правдой, потому что он так много узнал о системе безопас-

ности компании от доверчивого системного администратора. Если бы он

продолжил, то мог бы собрать достаточное количество маленьких частиц

информации, чтобы получить на их основе полный доступ к системе.

Настоящие сотрудники правоохранительных органов и персонал компании

предоставят информацию для проверки их личности, и они не будут противить-

ся, когда вы попросите их об этом.

Иногда потенциальные социальные инженеры разрабатывают свои планы,

начиная с информации, найденной в мусорных баках и мешках, что называет-

ся «мусорологией». Они ищут все, что может помочь им нанести ущерб вашей

компании: имена, номера телефонов или информацию о проектах.

Представьте, что злоумышленник находит в мусорном баке с бумагами компа-

нии бланк с упоминанием о таинственном «проекте Зет» в научно-исследова-

тельском отделе. К нему прикреплен список людей, работающих над проектом,

и их телефонных номеров. Злоумышленник воспользуется этим начальным

материалом и описанной тактикой телефонных звонков, чтобы получить от

ничего не подозревающих сотрудников все, что только можно. Такие люди

способны добиться очень приятного впечатления во время телефонного разго-

вора и могут достичь успеха, если сотрудники не будут бдительны. Злоумыш-

ленник может выдавать себя за нового сотрудника в проекте Зет, который ра-

ботает с [вставьте имя кого-либо указанного в списке] и пытается узнать, как

создать учетную запись, разобраться в подробностях удаленного доступа и т. д.

Как только учетная запись будет создана, человек сможет войти прямо в ваши

системы. Мораль этой истории заключается в том, что нужно сказать людям,

чтобы они были осторожны, разговаривая по телефону, и уничтожали докумен-

ты, которые могут содержать важную информацию, даже если они считают это

глупым.

Если вы обслуживаете интернет-шлюз своей организации, то вероятность того,

что с вами свяжутся сотрудники правоохранительных органов, гораздо выше.

Если правоохранительные органы связываются с вами регулярно, пора подумать

о рационализации процедур по работе с ними, чтобы избежать ошибок или

положения обвиняемого. Вы можете пройти обучение в юридическом отделе

и создать процедуру, которая позволит вам самостоятельно разбираться с ох-

ранниками правопорядка, и просто уведомлять юридический отдел о том, что

было их обращение. Таким образом, юридическому отделу не потребуется все

время направлять ваши действия. Конечно, исключительные случаи все равно

нужно передавать в юридический отдел. В лучшем случае проблема быстро

устраняется и в будущем жалобы не возникают. Однако у интернет-провайдеров

и компаний по веб-хостингу могут быть продолжительные цепочки проблем.

Основы

352

Не будьте слишком услужливы

Как-то раз одна компания запустила демоверсию веб-службы, которая

позволяла людям анонимно просматривать веб-страницы. Взломщики

пользовались этой службой, чтобы наносить ущерб другим сайтам.

К сожалению, правоохранительные органы сумели отследить сервер

с программой сохранения анонимности. Это было плохо. Когда возника-

ла проблема, правоохранительные органы связывались с системным

администратором, который передавал сообщение всем, кто пользовался

службой. После этого он забывал о проблеме, думая, что она решена. Его

интернет-соединение совместно использовали много служб, поэтому,

будучи типичным перегруженным работой системным администратором,

он только через некоторое время заметил, что многократные обращения

правоохранительных органов связаны с одной и той же службой.

Системный администратор беспокоился из-за недостатков службы, но

также хотел угодить своим клиентам. Он посоветовал группе, как изме-

нить службу, чтобы воспрепятствовать ее злонамеренному применению,

но группа не послушалась его. Скоро обращения правоохранительных

органов стали отнимать у него больше времени, так как его начали вы-

зывать в суд. Неудивительно, что он стал очень раздражительным

и сломался морально.

В конце концов он понял, что пытался решить эту проблему на непра-

вильном уровне. Он обратился к своему руководителю, и тот согласился,

что системный администратор не должен брать на себя ответственность

за проблемы, вызванные одним из его пользователей, особенно учитывая,

что он сделал эффективные предложения по исправлению службы. Он

имел полномочия для того, чтобы потребовать от пользователя исправ-

ления программного обеспечения, или отключить его в течение 30 дней.

Руководитель также решил, что лучше направлять обращения правоох-

ранительных органов в юридический отдел, чтобы обеспечить их более

грамотное рассмотрение.

Юридический отдел корпорации отключил службу в течение нескольких

минут после того, как узнал о ситуации, не дожидаясь, пока пройдет

целых 30 дней. Они были шокированы тем, что проблеме вообще позво-

лили существовать.

Все это говорит о том, что системный администратор должен был с само-

го начала жестче вести себя с клиентами. Если он не имел решительности или полномочий отключить клиента, то должен был передать про-

блему в юридический отдел, который обошелся бы с клиентом гораздо

суровее. Мораль этой истории – нужно быть строже с людьми, которые

вредят вашей компании, даже если они клиенты. Если они становятся

«хулиганами», лучше найти «хулигана» посильнее, который поможет

вам с ними справиться.

Вне зависимости от того, что вы думаете о правилах, вы обязаны выполнять

требования корпоративной службы безопасности. Если вы считаете эти требо-

вания неудобными, обратитесь к руководителю, не разбирайтесь в ситуации

сами.

Глава 12. Этика

353

Паника с логами принтера

С молодым системным администратором, который обслуживал систему

печати в крупной компании, связалась служба корпоративной безопасности. Для расследования дела о сексуальном домогательстве службе безо-

пасности требовались логи, связанные с тем, что было напечатано на кон-

кретном цветном принтере. Упомянутый принтер находился в здании,

в котором работал системный администратор, а это означало, что он может

знать подозреваемого. Системный администратор запаниковал. Он собрал

все логи с этого принтера и переписал их на свой компьютер дома. Затем

он удалил логи на работе. Наконец он обратился за советом к двум друзьям:

«Кого-то могут уволить! Что мне делать?» Оба друга дали ему один совет:

чтобы его самого не уволили, нужно восстановить логи и дать службе безо-

пасности то, что она требовала. Скрывая доказательства, он поставил себя

в опасное положение и стал выглядеть соучастником подозреваемого.

12.2. Тонкости

В данном разделе рассмотрено формирование ожиданий и несколько примеров

ситуаций, с которыми вы можете столкнуться.

12.2.1. Формирование ожиданий по неприкосновенности

личной информации и мониторингу

Установление политики неприкосновенности личной информации и монито-

ринга является принципиальным этическим вопросом. В данном разделе особое

внимание уделяется необходимости все время напоминать пользователям об

этой политике и ее последствиях.

Формирование ожиданий сотрудников в плане неприкосновенности личной

информации важно, потому что ставить людей в ситуацию, когда они не знают

законов, по которым живут, несправедливо. Наказывать людей за нарушение

правила, о котором им никогда не говорили, жестоко.

Есть много способов сформировать ожидания. При найме нужно потребовать от

сотрудников дать расписку в том, что они прочитали указания по неприкосно-

венности личной информации и мониторингу. Также компании могут требовать

от сотрудников давать такие расписки ежегодно. Время от времени компании

должны переиздавать положения о неприкосновенности личной информации

в сводках новостей или бюллетенях1. Размещение краткого содержания поли-

тики на видном месте или даже фраза «Все сеансы открыты для мониторинга»,

отображаемая на каждом экране входа в систему, может быть более эффектив-

ным, чем наличие длинной политики, находящейся на веб-сервере, на который

никто не заходит.

Оставлять сотрудников не информированными о правилах, касающихся непри-

косновенности личной информации, может быть опасно для бизнеса. Пользо-

Тонкости

1 Чтобы избежать путаницы в том, была ли политика изменена или просто пере-

издана, настаивайте на присвоении политикам номеров версий, а также указа-

нии дат.

354

ватели системы, которые не понимают, с какими рисками связаны их действия,

не могут управлять этими рисками. Представьте, что пользователи будут об-

суждать подробности патентованной деловой информации по электронной

почте, которую считают безопасной. Если она не является таковой, возможна

утечка информации. Из-за своей неосведомленности они подвергнут компанию

ненужному риску.

В финансовом сообществе электронная почта регулярно просматривается на

предмет нарушения норм Комиссии по ценным бумагам1, например биржевых

операций с использованием конфиденциальной (инсайдерской) информации.

Угроза просмотра может быть достаточной для предотвращения нелегального

обмена конфиденциальной информацией по электронной почте. Конечно, мож-

но просто перевести операции с использованием инсайдерской информации

обратно на каналы, которые труднее контролировать, например телефон. Од-

нако это решение принимается Комиссией по ценным бумагам, а не вами.

Компании электронной коммерции и любые компании, ведущие международ-

ный бизнес, должны обращать внимание на законы о неприкосновенности

личной информации, так как они различны в разных странах. Например, если

вы работаете с гражданами ЕС, есть строгие нормы относительно того, как вы

должны защищать личную информацию. Американские законы предполагают

аналогичную ответственность (см. раздел 12.1).

Формирование ожиданий также защищает репутацию системных администра-

торов, поскольку недостаток информации приведет к тому, что пользователи

будут предполагать худшее. Однажды у Тома был пользователь, который рань-

ше работал в компании, где системного администратора уволили за чтение

электронной почты других сотрудников. После этого пользователь считал, что

все системные администраторы читают чужую электронную почту. Однако

некоторые пользователи полагают, что электронная почта каким-то магическим

образом является безопасной, и подвергаются неразумному риску, отправляя

по электронной почте, например, данные о своих зарплатах. В компаниях, где

смотрят реально на компьютерные сетевые системы, наиболее важные данные

хранятся на сменных носителях – например, USB-«флэшках» или перезаписываемых CD/DVD, – а не размещают ее на сетевых файловых и почтовых серверах.

Так как сменные носители представляют собой простой способ для выноса дан-

ных с территории компании либо могут быть утеряны или украдены во время

транспортировки, политика должна касаться и этих вопросов. Например,

у продавцов очень распространено копирование своей адресной книги элект-

ронной почты и списка контактов на сменный носитель для дополнительного

резервного копирования. Также часто случается, что эти резервные копии ос-

таются у них после увольнения, хотя политики запрещают оставлять конфи-

денциальную информацию, просто потому, что «все так делают». Если ваша

политика устанавливает другую планку, убедитесь, что руководство хочет ее

поддерживать.

1 В России это ФСФР, Федеральная служба по финансовым рынкам. – Примеч.

науч. ред.

Глава 12. Этика

355

Пример: перенаправление электронной почты

В компании была либеральная политика, разрешающая перенаправление

электронной почты бывших сотрудников на их новые адреса электронной

почты в течение года. Политика создавала проблемы, потому что конфи-

денциальная деловая информация часто массово рассылалась по спискам,

которые не обновлялись с целью удалить уволенных сотрудников. Все

думали, что электронная почта внутри компании была безопасной, даже

если сообщения рассылались по всему подразделению. Пока всем в ком-

пании не рассказали об этой проблеме, сотрудники не знали, что они

рисковали безопасностью, рассылая массовые сообщения.

Лучшая политика – установить системы автоматического ответа с сооб-

щением, включающим новый адрес электронной почты человека и явное

указание, что сообщение отправителя не было перенаправлено. К сожа-

лению, из-за угрозы сбора адресов электронной почты спамерами сейчас

лучше просто указать, что учетная запись была удалена, и не писать

никакого нового адреса электронной почты.

Сейчас у людей часто имеется личная электронная почта вне работы,

поэтому такое уведомление уже не является необходимым.

12.2.2. Указание поступить незаконно/безнравственно

Ни одна глава об этике не была бы полной без обсуждения вопроса, что делать,

если ваш руководитель просит вас совершить что-то незаконное, безнравствен-

ное или противоречащее правилам компании. Мы надеемся, что вам никогда

не понадобится информация этого раздела, но лучше быть подготовленным

и понимать потенциальные проблемы, чем быть застигнутым ими врасплох.

Самое важное, что нужно помнить в этой ситуации, – необходимо записывать

события. Ведите записи, отражающие, когда делаются такие требования, когда

происходят связанные с ними телефонные звонки, какие команды вы вводите

для их выполнения и т. д. Записи – ваш друг.

Мы рекомендуем простой процесс: проверьте требование – может быть, вы не-

правильно его поняли; проверьте, является ли оно незаконным или противоре-

чащим политике компании, – посмотрите в политике или спросите у кого-нибудь

совета; если требование противоречит политике, вежливо отстаивайте свою

точку зрения и открыто откажитесь выполнять требования.

Если руководитель настаивает, вы можете согласиться с ним, обратиться

к вышестоящему руководству или сделать и то и другое одновременно. Во мно-

гих компаниях есть уполномоченный по рассмотрению жалоб, с которым вы

конфиденциально сможете обсудить такие ситуации. В жестко регулируемых

отраслях, например в финансовой сфере, есть четко определенные указания,

что делать дальше. Даже в небольшой фирме у вас есть возможность обратить-

ся в отдел кадров или юридический и сообщить, что вы в ситуации, в которой

вам требуются указания.

Тонкости

356

Полезный прием – попросить оформить требование в письменной форме или

в виде сообщения электронной почты. Это дает вам документ и заставляет че-

ловека письменно подтвердить свое требование. Если требование было право-

мерным, но неправильно понятым, его просмотр в сообщении электронной

почты может прояснить ситуацию.

Человек, требующий чего-то безнравственного и знающий об этом, не оформит

это в письменном виде. Это может положить конец сомнительному требованию.

Однако трудно попросить оформить требование в письменной форме, чтобы это

не звучало конфронтационно. Для большинства руководителей просьба повто-

рить требование в письменном в виде или по электронной почте звучит как

неподчинение. Вместо этого вы можете попросить: «Не могли бы вы мне отпра-

вить по почте напоминание, чтобы я смог посмотреть ваше требование после

обеда?» Если человек не согласится, вы можете сказать, что сообщение требу-

ется вам, чтобы удостовериться в том, что вы правильно понимаете требование.

Если и это не получится, вам придется раскрыть свои карты: «Либо я не понимаю

вашего требования, либо вы требуете от меня сделать что-то сомнительное».

Затем предложите, чтобы к беседе присоединился кто-то еще, например ваш

руководитель, руководитель вашего руководителя или любой другой, кого это

напрямую касается.

Просьба прочитать чью-то электронную почту

Давайте рассмотрим эту ситуацию на вымышленном примере: начальник отде-

ла Боб просит вас прочитать электронную почту начальника отдела Элис, чтобы

узнать, не планирует ли ее отдел отменить проект, на который сильно рассчи-

тывает отдел Боба. Хорошим ответом будет переспросить, чтобы убедиться, что

вы поняли просьбу правильно: «Что вы просите меня сделать?»

Если требование подтверждается, проверьте, противоречит ли оно политике

компании, найдите соответствующий пункт в указаниях вашей организации

по неприкосновенности личной информации и мониторингу. Вежливо проверь-

те, понимает ли человек, что просит поступить безнравственно: «Может быть,

я вас не расслышал?1 Вы имеете в виду, что я должен…», и укажите, что это

противоречит политике.

Воспользуйтесь политикой для вежливого напоминания Бобу. Боб может рационально обосновать свою просьбу, объясняя, что Элис отменила другие реше-

ния и что он пытается только помочь вам, потому что знает, что вы тоже рас-

считываете на этот проект.

На этом этапе вам нужно принять решение. Вы можете временно уйти от ответа

и поговорить с уполномоченным по рассмотрению жалоб, сотрудником службы

корпоративной безопасности или руководителем Боба. Вы можете согласиться

с требованием, но это делает вас соучастником. В дальнейшем Боб может потребовать чего-то еще, возможно, намекнув, что, если вы не согласитесь, он

расскажет о предыдущем случае, утверждая, что вы сделали это по своей ини-

циативе. Он также может утверждать, что, если вы не согласитесь, он просто

найдет кого-то еще, кто это сделает. Эта тактика является очень опасной для

того, кто пытается убедить человека что-то сделать.

Очевидно, что мы не можем принять решение за вас. Однако мы можем дать вам

следующий совет: когда вы сомневаетесь, следует ли вам что-то делать, полу-

Глава 12. Этика

1 Или, если требование было сделано по электронной почте, «Я думаю, что мог

что-то перепутать или неправильно понять вашу просьбу…».

357

чите требование в письменной форме и записывайте, что конкретно вы делаете.

Никогда не действуйте по устным указаниям, которые считаете сомнительны-

ми. Даже если вы думаете, что все может быть нормально, получите требование

в письменном виде. Это важно не только для того, чтобы оградить себя, но и для

того, чтобы помочь человеку, выдвигающему требование, удостовериться в том,

что он действительно этого хочет. Если человек не хочет давать требование

в письменном виде, то он не желает нести за него ответственность. В ваших

записях должно быть указано время, требование, кто его сделал, почему это

было сделано и что было сделано. Кроме того, отмечайте все необычное, что

касается требования. Обычно люди жалеют о том, что не вели записи, когда уже

слишком поздно. Логи с автоматическими временными метками обеспечивают

лучшую отчетность и исключают утомительность ведения записей.

12.3. Заключение

Этика – это принципы поведения, которые регулируют действия людей. Для

многих людей само слово «этика» является неопределенным и пугающим. На-

деемся, что мы предоставили вам несколько руководящих принципов, которы-

ми вы можете воспользоваться, и не ущемили вашу свободу сделать свой собственный выбор.

Этический кодекс системного администратора направлен на повышение про-

фессионализма и улучшение имиджа системных администраторов, он устанав-

ливает стандарт поведения. Политики, которые создает организация, должны

включать нормы поведения пользователя сети/компьютера, нормы поведения

пользователя с привилегированным доступом, политику соблюдения авторских

прав и политику работы с правоохранительными органами. Принцип согласия,

основанного на полученной информации, определяет, что у нас должна быть

политика мониторинга и неприкосновенности личной информации, в явном

виде доведенная до всех пользователей. В случае отсутствия санкций за нару-

шения и последовательной поддержки эти политики бесполезны.

Предварительное обдумывание возможных ситуаций помогает вам лучше под-

готовиться к ним. Постарайтесь подумать о потенциальных этических дилем-

мах, с которыми вы можете столкнуться, и о том, что вы будете делать в этих

случаях. Это может быть хорошей темой для периодического обсуждения на

собраниях персонала или во время обеда. Оно должно проходить в присутствии

вашего руководителя, чтобы вы могли способствовать пониманию официальной

политики.

Надеемся, главное, что вы усвоили из этой главы, – это следующее: если вы

находитесь в непонятной ситуации, лучший способ защитить себя – вести за-

писи. Просите оформить требование в письменной форме, чтобы создать запись

о нем, записывайте, когда вы получаете телефонные звонки, записывайте, что

вас просят делать и что вы делаете. Записывайте все!