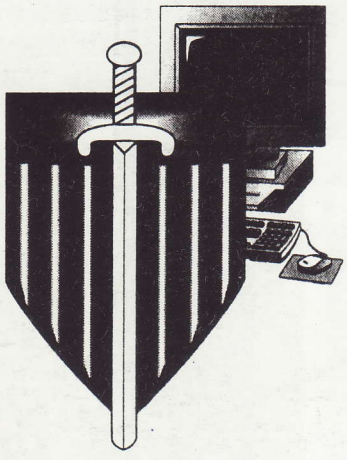
Jet INFO

МАТЕРИАЛ НОМЕРА

Руководство по информационной безопасности предприятия



А ТАКЖЕ:

- **ПРАКТИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**
- **СВОДНЫЕ ДАННЫЕ О ВЫДАЧЕ СЕРТИФИКАТОВ ГОСТЕХКОМИССИЕЙ РОССИИ**

10/11 1996

ИНФОРМАЦИОННЫЙ БЮЛЛЕТЕНЬ

АКТУАЛЬНАЯ ТЕМА

Сергей Вихорев, Александр Ефимов
Гостехкомиссия России

Практические рекомендации по информационной безопасности

Содержание

1. Введение

В 1992 году Указом Президента Российской Федерации вместо существовавшей около 20 лет Государственной технической комиссии СССР была образована Государственная техническая комиссия при Президенте Российской Федерации (Гостехкомиссия России) – коллегиальный орган, отвечающий в том числе и за координацию усилий в области защиты информации. Сейчас, когда эта проблема становится все более актуальной, в Гостехкомиссию России постоянно поступают запросы от организаций различных форм собственности о порядке и правилах защиты информации в Российской Федерации. Не претендуя на полный и детальный анализ положения дел в данной области (это труд, достойный отдельной монографии), авторы попытались осветить основные вопросы, которые возникают перед руководителями и сотрудниками служб безопасности на начальном этапе процесса обеспечения защиты информации.

2. Информация и ее виды

Деятельность любого учреждения включает в себя получение информации, ее обработку, принятие решений на основе анализа информации и передачу принятых решений по каналам связи. Искажение информации, блокирование ее получения или внедрение ложной информации, способствуют принятию ошибочных решений.

Информация – это специфический продукт, поэтому необходимы четкие границы, определяющие информацию как объект права, которые позволят применять к ней законодательные нормы.

Федеральный Закон "Об информации, информатизации и защите информации", направленный на регулирование взаимоотношений в информационной сфере совместно с Гражданским кодексом Российской Федерации, относит информацию к объектам права и дает ее определение:

"Информация – сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления".

Основными целями защиты информации, согласно Закону, являются:

- предотвращение утечки, хищения, искажения, подделки информации;
- обеспечение безопасности личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, искажению, блокированию информации;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных;
- сохранение государственной тайны, конфиденциальности документированной информации.

По этому Закону защите подлежит информация ограниченного доступа, а степень ее защиты определяет собственник этой информации. Ответственность за выполнение мер защиты лежит не только на собственнике, но и на пользователе информации. Значит, прежде всего необходимо уяснить, используется ли в Вашем учреждении информация, быть может, Вам и не принадлежащая, но подлежащая обязательной защите.

Отметим, что защищается только документированная информация. Федеральный Закон "Об информации, информатизации и защите информации" определяет это понятие следующим образом:

"Документированная информация (документ) – зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать".

Документирование информации проводится по строго определенным правилам. Основные из них изложены в ГОСТ 6.38-90 "Система организационно-распорядительной документации. Требования к оформлению документов.", ГОСТ 6.10.4-84 "Унифицированные системы документации. Придание юридической силы документам на машинном носителе и машиног-

рамме, создаваемым средствами вычислительной техники.".

Надо отметить, что эти ГОСТы предполагают 31 реквизит, который делает информацию документом. Не обязательно, чтобы присутствовали сразу все реквизиты. Главным из них является текст документа, поэтому любая информация, изложенная в виде связного текста, без каких-либо дополнительных реквизитов уже может рассматриваться как документ. В то же время, для придания документу юридической силы одного текста недостаточно. Необходимы также такие важные реквизиты, как дата и подпись.

Для документов, полученных из автоматизированных информационных систем, существует особый порядок придания им юридической силы. При этом, в определенных случаях, применяется процедура заверения информации электронной подписью.

Защита информации — удовольствие дорогое, поэтому одним из принципов построения системы защиты должен стать принцип разумной достаточности, требующий учета степени важности и ценности защищаемой информации.

Закон выделяет три категории такой информации:

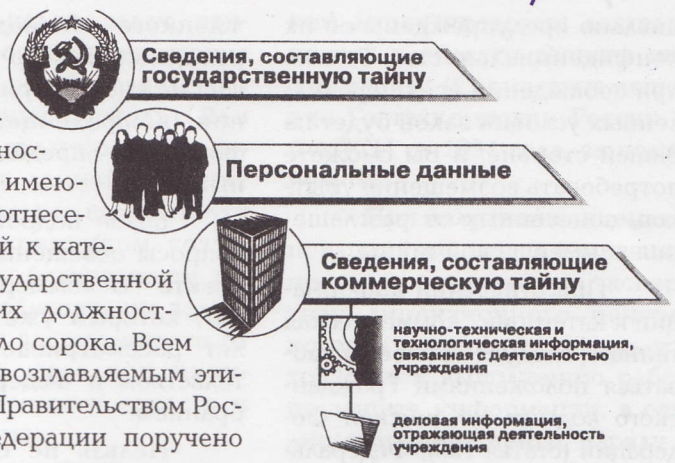
- информация, составляющая государственную тайну;
- персональные данные;
- информация, составляющая коммерческую тайну.

Информацией первой категории владеет само государство и, естественно, именно оно выдвигает требования по ее защите и контролирует их выполнение. Соответствующие положения закреплены в Законе Российской Федерации "О государственной тайне", принятом в 1993 году. Следует знать, что нарушение этих требований влечет за собой применение санкций, предусмотренных Уголовным кодексом.

В настоящее время разработан Перечень должностных лиц, имеющих право отнесения сведений к категории государственной тайны. Таких должностных лиц около сорока. Всем ведомствам, возглавляемым этими лицами, Правительством Российской Федерации поручено разработать конкретные перечни сведений, составляющих государственную тайну, которые являются развитием общероссийского Перечня. Такой перечень сформирован Гостехкомиссией России, согласован с заинтересованными министерствами и ведомствами и представлен в Правительство Российской Федерации. До его утверждения, наверное, рано говорить о его широком опубликовании, однако, всегда можно получить исчерпывающую консультацию по вопросу отнесения сведений к категории государственной тайны, обратившись непосредственно в Гостехкомиссиию России или соответствующие министерства и ведомства.

Собственниками второй категории информации являемся мы с Вами, так как эта информация затрагивает нашу с Вами личную жизнь. Однако, понимая степень значимости этой информации и ее роль в обеспечении безопасности каждой отдельно взятой личности, государство взяло ее под свой патронат и рассматривает ее защиту, как одну из своих важных задач.

К сожалению, правовая сторона этого вопроса на современном этапе проработана недостаточно. Только Закон "Об информации, информатизации и защите информации" относит персональную информацию к категории конфиденциальной и требует ее защиты наравне с информацией, составляющей государственную тайну, однако дальнейшего развития эти положения, в том числе и в плане конкретной ответственности за разглашение персональных данных, их утрату или искажение, пока не получили. Будем надеяться, что находящийся в настоящее время в Правительстве Российской Федерации законопроект "О персональных данных", который планируется рассмотреть и представить в Государственную Думу, решит эти вопросы.



Информацией третьей категории владеют сами учреждения, и поэтому они вправе ей распоряжаться, а, следовательно, и выбирать степень ее защиты. Правда, применить какие-либо санкции в случае нарушения конфиденциальности возможно, только если предварительно были выполнены особые формальности, оговоренные Гражданским кодексом Российской Федерации.

Суть этих формальностей, изложенных в статье 139 Гражданского кодекса Российской Федерации, заключается в том, что, во-первых, информация должна иметь действительную или потенциальную коммерческую ценность, во-вторых, учреждению необходимо принять определенные меры по охране конфиденциальности и, в-третьих, все сотрудники, знакомые с этими сведениями, должны быть офи-

циально предупреждены об их конфиденциальности. Только при соблюдении всех перечисленных условий закон будет на Вашей стороне, и Вы сможете потребовать возмещения убытков, понесенных от разглашения коммерческой тайны.

При отнесении информации к категории "коммерческая тайна" следует руководствоваться положениями Гражданского кодекса Российской Федерации (статья 139), Федерального Закона "Об информации, информатизации и защите информации" (часть 3, статья 10) и Постановления Правительства Российской Федерации от 5 декабря 1991 года за номером 35 "О перечне сведений, которые не могут составлять коммерческую тайну"

Сведения, относимые к категории "коммерческая тайна", можно разделить на две группы:

- Научно-техническая и технологическая информация, связанная непосредственно с деятельностью учреждения, то есть конструкторская и технологическая документация, сведения об используемых материалах, описание методов и способов производства разрабатываемых изделий, специфический или уникальный программный продукт, перспективные планы развития или модернизации производства;
- Деловая информация о деятельности учреждения, то есть финансовая документация, перспективные планы развития, аналитические материалы об исследованиях конкурентов и эффективности работы на рынке товаров и услуг, различные сведения о партнерах и т.п.

Чтобы отнесение к категории коммерческой тайны приобрело законную силу, оно должно быть оформлено в виде специального перечня, утвержденного руководителем учреждения, Только в этом случае можно говорить о придании конфиденциальной информации определенных вещных прав.

Более подробно все эти вопросы освещены в законопроекте "О коммерческой тайне", который уже более двух лет рассматривается Правительством и Федеральным собранием.

Нельзя не сказать и о том, что Гражданским кодексом Российской Федерации информация наделена правами товара. Она может представлять определенную ценность (даже не относясь к вышеперечисленным категориям), обмениваться, продаваться, дариться и т.п., поэтому, оценивая информацию с точки зрения важности ее защиты, следует учитывать и этот аспект.

Мы видим, что законодательство в области защиты информации пока далеко от совершенства, однако, при правильном использовании имеющихся законодательных и целого ряда подзаконных актов, можно добиться возмещения убытков, явившихся следствием нарушения режима информационной безопасности, и, в то же время, не попасть под карающий меч государства.

Совет 1. Проанализируйте информацию, которая циркулирует в Вашем учреждении, выделите информацию ограниченного доступа, определите круг информации, составляющей государственную тайну, оцените коммерческую важность информации. Все это позволит Вам дифференцировать мероприятия по обеспечению безопасности информации и, тем самым, сократить расходы. Не забудьте утвердить Перечень сведений, составляющих коммерческую тайну, и ознакомить с ним исполнителей.

3. Возможные угрозы информационной безопасности

Есть много способов нелегального получения информации или ее искажения. Можно, например, сфотографировать важный документ, украсть папку с документами или дискету с информацией, перехватить излучения электронных устройств, обрабатывающих информацию, и т.д.

Угрозы делятся на внешние и внутренние, причем последние представляют особую опасность. Поэтому, прежде всего убедитесь в лояльности персонала Вашего учреждения. Принимая сотрудника на работу, постарайтесь всеми доступными средствами навести о нем справки. Примените специальные психологические тесты, которые помогут оценить его лояльность и психологические качества. Продумайте систему материального и морального поощрения за сохранение лояльности. Регулярно проверяйте по специальным тестам сотрудников, которые соприкасаются с информацией ограниченного доступа.

Если Вы используете информацию, составляющую государственную тайну, то большинство этих вопросов решится само по себе, когда Ваши сотрудники будут оформлять соответствующий допуск. Но если подобной информации у Вас нет, то решение этих проблем — Ваша забота. Обязательно оговорите в контракте с сотрудником условия сохранения конфиденциальности не только на период совместной работы, но и на определенный срок после завершения ваших взаимоотношений. Только в этом случае Вы сможете предъявлять какие-либо претензии.

Совет 2. Проповедуйте принцип "доверяй, но проверяй". До нача-

ла построения системы безопасности Вашего учреждения в целом и безопасности информации в частности, убедитесь в лояльности Ваших сотрудников и, особенно, сотрудников службы безопасности. Примите необходимые меры морального и материального плана для поощрения их лояльности — это вселит в Вас уверенность, что в критический момент система безопасности не подведет.

Старайтесь придерживаться комплексного подхода к решению проблемы защиты информации. Для того, чтобы риск Вашей коммерческой деятельности был минимальным, надо оценить всевозможные угрозы безопасности информации с учетом двух факторов: предполагаемой вероятности возникновения угрозы и возможного ущерба от ее осуществления. Объективность оценки угроз достигается детальным анализом функционирования Вашего учреждения и привлечением независимых экспертов.

4. Концепция безопасности

Анализ мирового и отечественного опыта диктует необходимость создания целостной системы безопасности учреждения, увязывающей оперативные, оперативно-технические и организационные меры защиты, использующей современные методы прогнозирования, анализа и моделирования ситуаций. Эта система должна существовать и выполнять свои функции не один год. Однако, постоянно меняющаяся политическая, социальная и экономическая ситуация не позволяет заранее предусмотреть все возможные варианты и ограничиться фиксированным набором мер защиты. Поэтому-то Вам и нужна концепция обеспечения безопасности учреждения, представляющая собой систематизированное изложение целей, задач, принципов и способов достижения информационной безопасности. Концепция позволит Вам правильно спланировать деятельность в данной области. При этом следует помнить, что основным принципом создания системы безопасности должно стать обеспечение заданного уровня защищенности от возможных угроз при минимальной стоимости средств и систем защиты.

Совет 3. Первым шагом к решению проблемы защиты информации должно стать создание концепции информационной безопасности и ее увязывание с общей концепцией безопасности Вашего учреждения.

Концепция представляет собой официально принятую систему взглядов на проблему информационной безопасности и пути ее решения. Она является методологической основой практических мер по ее реализации.

Разработка концепции — это кропотливая научная работа, поэтому целесообразно поручить ее людям, профессионально занимающимся данным вопросом. Государство, понимая важность этого направления, на законодательном уровне ввело контроль за деятельностью предприятий в области защиты информации. Этот контроль осуществляется через государственное лицензирование, которое проводит Гостехкомиссия России в части оказания услуг по защите информации, изготовлению и реализации средств защиты информации и защищенных технических средств, и ФАПСИ в части оказания услуг и применения средств криптографии. Перечень видов деятельности, подлежащих лицензированию, довольно широк, а порядок лицензирования определяется "Положением о государственном лицензировании деятельности в области защиты информации" (Совместное решение Гостехкомиссии России и ФАПСИ от 1994 года, за номером 10).

При получении лицензии предприятие или организация проходит специальную экспертизу лицензионного центра, которая позволяет оценить готовность к выполнению работ по защите информации, а сам лицензионный центр, наряду с лицензиатом, несет юридическую ответственность за качество выполняемых работ и конфиденциальность используемой информации. Это служит гарантией качества тех услуг, которые указаны в лицензии.

Совет 4 Поручайте работы в области защиты информации только предприятиям и организациям, имеющим Лицензию Гостехкомиссии России — это гарантирует Вам высокое качество работ и позволит в случае необходимости применить юридические санкции.

5. План практических мероприятий

Приступая к составлению плана практических мероприятий, необходимо прежде всего, на основе оценки уже имеющейся технической базы и исследования применяемого программного обеспечения, решить вопрос об оснащении или, может быть, переоснащении учреждения специальными средствами безопасности, защищенными техническими средствами, средствами защиты и контроля. Цель этих действий — определить методы и способы включения в уже существующую информационную систему средств защиты информации. Уязвимые точки этой системы определены в концепции, так что осталось "только" подобрать такие средства, которые удовлетво-

рили бы Вас по стоимости и эффективности.

Не вызывает сомнений, что для эффективной защиты информации нужны средства, которые соответствуют определенным требованиям. Законом "Об информации, информатизации и защите информации" вводится обязательная государственная сертификация средств обработки информации и ее защиты. Наличие сертифицированных средств дает Вам преимущества при проведении страхования информации.

На защиту интересов владельцев информации — основных потребителей товаров и услуг в области ее защиты — нацелены "Система сертификации средств защиты информации по требованиям безопасности информации" (РОСС RU 0001. 01БИ00) и "Система сертификации средств криптографической защиты информации (СКЗИ)" (РОСС RU 0001.03001).

Сертифицируются защищенные технические, программно-технические, программные средства, системы, сети вычислительной техники и связи, средства защиты и средства контроля эффективности защиты. Если Вы в своей работе используете информацию с ограниченным доступом, то Ваши средства, в том числе и иностранного производства, должны пройти обязательную сертификацию. В остальных случаях сертификация носит добровольный характер.

Совет 5. Применяйте для обработки информации ограниченного доступа только аппаратные и программные продукты, имеющие сертификат, выданный Гостехкомиссией России, для программных и технических средств защиты информации, не использующих методы криптографии, и сертификат ФАПСИ — для средств защиты с применением криптографии.

Система сертификации средств защиты по требованиям безопасности информации создана недавно. Сейчас идет активный процесс сертификации. Многие производители, понимая рыночные преимущества сертифицированных продуктов, подали заявки на проведение испытаний. Вместе с тем, на сегодня уже имеется много программных и технических средств, прошедших сертификацию. В их числе есть и специальные программы, обеспечивающие защиту от несанкционированного доступа, и защищенные технические средства зарубежных и отечественных производителей, и специальные средства защиты от перехвата побочных электромагнитных излучений и наводок и многое другое.

Перечни средств защиты, прошедших сертификацию, постоянно обновляются и рассылаются Гостехкомиссией России во все администрации регионов и заинтересованные министерства. Есть эта информация и в Госсандарте России, который ведет сводный перечень средств, имеющих различные сертификаты. Кроме того, за консультацией можно обратиться непосредственно в Гостехкомиссию России.

Помните, что выставить продукцию на сертификацию может не только производитель, но и потребитель. Для этого необходимо подготовить заявку в федеральный орган по сертификации, каковым для программных и технических средств защиты информации, не использующих методы криптографии, является Гостехкомиссия России. Эта заявка будет рассмотрена и передана в одну из испытательных лабораторий, аккредитованную в Системе сертификации. Дальше все ясно — испытания, отчет, рассмотрение результатов экспертной комиссией и, при положительном заключении, получение сертификата от федерального органа. Правда, в этом случае сертификат выдается на единичный образец продукции. Но иногда, особенно если Вы в своей работе используете уникальный программный или технический продукт, расходы на сертификацию будут оправданы.

После того, как выбраны и закуплены все необходимые технические и программные средства защиты, завершены работы по их монтажу и наладке, необходимо провести комплексную проверку эффективности принятых мер. Такая проверка проводится по известным методикам и предусматривает моделирование различных реальных ситуаций и оценку возможности несанкционированного получения информации. Для проведения проверки лучше всего воспользоваться услугами организации, располагающей соответствующей лицензией.

Совет 6. Убедитесь в достаточности принятых мер, проведя проверку эффективности средств защиты.

Информационная безопасность организации зависит не только от технических средств, но и от людей, их использующих. Если дать самый лучший инструмент в руки неопытного человека, можно только навредить делу. Следует, во-первых, научить сотрудников пользоваться защитными средствами. На каждом рабочем месте должны быть инструкции и памятки, в доступной форме информирующие персонал об обязательных мерах по поддержанию информационной безопасности.

Во-вторых, Вам необходимы специалисты, способные грамотно обслуживать систему защиты. Чтобы подготовить таких специалистов, отберите нескольких наиболее подготовленных сотрудников и направьте их на дополнительное обучение в один из учебных центров Гостехкомиссии России. Такое обучение может длиться от 2 недель до 3 месяцев.

Если Вы только набираете сотрудников, обратите внимание на выпускников МИФИ, МГТУ им. Н.Э. Баумана. Эти ВУЗы готовят специалистов нужного Вам профиля. Не надо забывать и о старых кадрах. Вопросами защиты информации профессионально занимались и занимаются специалисты спецподразделений предприятий оборонного комплекса, военных и некоторых других организаций.

Совет 7. Организуйте подготовку персонала по вопросам защиты информации. Разработайте и доведите до каждого правила информационной безопасности.

6. Заключение

В результате выполнения предложенных мероприятий следует ожидать качественно более высокого уровня безопасности, снижения страховых платежей за счет повышения защищенности бизнеса от различных видов угроз, предотвращения ущерба от противоправных действий злоумышленников и конкурентов. Затратив сегодня определенные средства на обеспечение безопасности информации, Вы уже завтра получите выгоду.

Приложение. Какие законы следует знать и применять

1. Гражданский кодекс Российской Федерации.
2. Федеральный Закон "Об информации, информатизации и защите информации".
3. Федеральный Закон "О связи".
4. Закон Российской Федерации "О государственной тайне".
5. Закон Российской Федерации "О защите прав потребителей".
6. Закон Российской Федерации "О сертификации продукции и услуг".
7. Закон Российской Федерации "О федеральных органах правительственной связи и информации".
8. Указ Президента Российской Федерации от 1992 года за номером 9 "О создании Государственной технической комиссии при Президенте Российской Федерации".
9. Указ Президента Российской Федерации от 1995 года за номером 334 "О мерах по соблюдению законности в области разработки, производства, реализации и эксплуатации шифровальных средств, а также предоставления услуг в области шифрования информации".
10. Постановление Правительства Российской Федерации от 1994 года за номером 1418 "О лицензировании отдельных видов деятельности".
11. Постановление Правительства Российской Федерации от 1995 года за номером 333 "О лицензировании деятельности предприятий и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны".
12. Совместное решение Гостехкомиссии России и ФАПСИ от 1994 года за номером 10 "Положение о государственном лицензировании деятельности в области защиты информации".
13. "Система сертификации средств защиты информации по требованиям безопасности информации". – РОСС RU.0001.01БИ00.
14. "Система сертификации средств криптографической защиты информации (СКЗИ)". – РОСС RU 0001.03001.

СВОДНЫЕ ДАННЫЕ О ВЫДАЧЕ СЕРТИФИКАТОВ ГОСТЕХКОМИССИЕЙ РОССИИ

по состоянию на 1 февраля 1996 года

N п/п	Дата выдачи и N сертиф.	Срок действия	Шифр изделия	Назначение изделия	Вид изделия	Заявитель	Адрес, телефон
1	12.08.93 N 1	5 лет	"Снег 1.0"	Система защиты информации от НСД для ПЭВМ IBM PC XT/AT. В нее входит СКЗД "Иней".	Программно-техническое	ЦНИИАтоминформ МИНАТОМА РОССИИ	127434,Москва, а/я 971 т.210-8256, 210-8001, 210-8877
2	12.08.93 N 2	5 лет	"Снег-ЛВС"	Система защиты информации от НСД в ЛВС. В нее входит СКЗД "Иней-ЛВС". Заказ к НИР "Андор".	Программно-техническое	ЦНИИАтоминформ МИНАТОМА РОССИИ	127434,Москва, а/я 971 т.210-8256, 210-8001, 210-8877
3	02.08.93 N 3	3 года	"УралВЭС"	Закрытая часть электронного почтамта центрального узла сети "УралВЭС".	Программно-техническое	ТОО "Микротест"	620219,Екатеринбург, ГСП-141, ул.Мамина-Сибиряка, 85
4	09.11.93 N 4	7 лет		Встроенная система парольной защиты загрузки ПЭВМ PCD-4 Gsx/25 фирмы Simens Nixdorf.	Программно-техническое	Управление информационных ресурсов Администрации Президента	
5	28.02.94 N 7	2 года		Техническая доработка ПЭВМ в целях снижения уровня ПЭМИН.	Техническое	НП концерн "Научный центр"	103460, Москва, Зеленоград, НПК "Научный центр"
6	08.08.94 N 9	до 31.12.94	МП-1	Устройство блокировки канала утечки речевой информации в телефонных аппаратах (аналог "Гранит-VIII").	Техническое	ТОО фирма "Юрвек",	103626, Москва, Б.Черкасский пер., 13
7	04.10.94 N 10	до 31.12.94		Техническая доработка персональных ЭВМ IBM PS-1 в целях снижения уровня ПЭМИН.	Техническое	АО "РНТ",	103009,Москва, Тверская,12/7, офис 267 т.209-2957;209-6293
8	15.11.94 N 11	до 15.05.95	изд.83т744	Программно-техническая доработка изделия 83т744 от НСД к информации.	Программно-техническое	НИИ АА	г. Москва
9	07.12.94 N 13	до 31.05.95	"Агат"	Устройство защиты от прослушивания телефонных аппаратов при положенной на рычаги микротелефонной трубке.	Техническое	ТОО "Экста" г.Зеленоград	103498, Москва, а/я 433-48 т.536-9621

N п/п	Дата выдачи и N сертиф.	Срок действия	Шифр изделия	Назначение изделия	Вид изделия	Заявитель	Адрес, телефон
10	09.12.94 N 14	до 31.05.95	IPC POS IIS # P	Автоматизированный кассовый аппарат на базе ЭВМ IBM PC с системой защиты и разграничением доступа.	Программно-техническое	Фирма "ПИЛОТ"	121458, Москва, Каширское ш., 32/2 т.923-0127
11	28.12.94 N 15	до 31.12.95	Аккорд	Единичный образец прогр.-апп. комплекса "Аккорд" (СТЮИ.00506-01 ТУ). Защита ПЭВМ от НСД. (Таблетка)	Программно-техническое	ОКБ САПР	113114,Москва, 2 Кожевнич.пер. 4/6.т.235-1606
12	27.01.95 N 16		ГШ - 1000	Средство активной защиты - генератор шума с диапазоном частот от 0.1 до 1000 МГц	Техническое	ЦНИИМаш РКА	141070,Калининград Моск обл., ул.Пионерская,4 т.513-5000
13	27.09.95 N 17	до 31.12.98	ФСПК-200(100)	Защитное устройство подавления опасных сигналов в однофазных и трехфазных сетях электропитания	Техническое	ГЦИПК и НПП "Элком"	249020,Обнинск, Калужской обл., ул.Курчатова,21
14	14.02.95 N 18	до 14.08.95	"УЗТ"	Устройство защиты от прослушивания помещения через телефонный аппарат, находящийся в режиме ожидании вызова	Техническое	ТОО "Предприятие ЛиК"	127106, Москва, Ботаническая ул., 25
15	15.02.95 N 19	до 31.05.95	АСБН "БЛИЦ"	Автоматизированная система безналичных расчетов "БЛИЦ", функционирующая совместно с СЗИ от НСД QP DOS TK	Программно-техническое	АОЗТ "БЛИЦ-ЦЕНТР"	121019, Москва, ул.Грицевецкая, 8/12,стр.4
16	22.06.95 N 20	до 31.12.98	"Кобра"	Система защиты информации от НСД для ПЭВМ (по 4-ому классу защищенности)	Программное	ГНИИ модел. и интеллект. слож ных сист. и АОЗТ "Кобра-ЛАЙН"	197376,С-Петербург, ул. проф.Попова, 5, ИМИСС т. 234-9094;234-9093 т. 272-7465
17	29.09.95 N 21	до 31.12.98	"Страж 1.1	Программный комплекс защиты информации от НСД для ПЭВМ (по 2-ому классу защищенности)	Программное	в/ч 01168	123007, Москва,1-й Хорошевский, пр., д. 3 т.945-7175, 293-9612
18	10.11.95 N 22	до 31.12.98	"Марс"	Комплекс программных средств защиты от НСД для персонального компьютера "МАРС" (КПСЗИ "МАРС") — по 3 классу защищенности	Программное	Российский центр "Безопасность"	109316, Москва,Волгоградский проспект, 16 т.978-9303, 978-9155 , 288-3788

N п/п	Дата выдачи и N сертиф.	Срок действия	Шифр изделия	Назначение изделия	Вид изделия	Заявитель	Адрес, телефон
19	05.12.95 N 23	до 31.12.98	"Виконт"	Телевизионная система наблюдения	Техническое	НПО "Альфа-Прибор"	300000, Тула, а/я 464 т.(0872)31-2755, 36-1815 31-2755
20	25.12.95 N 24	до 31.12.98	"Кютак-С"	Автоматизированный программно-аппаратный комплекс по управлению и расчетам автозаправочных предприятий	Программно-техническое	АО "Центр технич. обслуж. ККМ"	196084,С-Петербург, ул.Заставная,33 т.(812)272-3259, 272-2206
21	25.12.95 N 25	до 31.12.98	ГШ-К-1000	Средство активной защиты - генератор шума с диапазоном частот от 0.1 до 1000 МГц	Техническое	СКБ ИРЭ РАН	141120,Фрязино, Моск.обл., пл.ак. Введенского,1 т.(095)526-9233
22	25.12.95 N 26	до 31.12.98	"Салют"	Устройство защиты ПЭВМ от перехвата ЭМИиН объектов ВТ 2,3 категорий в диап частот 10-1000 МГц (ИТСВ.469 435.006-02 ТУ)	Техническое	ТОО "НТФ"Криптон"	117420, Москва, ул.Профсоюзная, д. 78 т.(095)330-6283 330-5192
23	25.12.95 N 27	до 31.12.98	"Корунд"	Устройство защиты от прослушивания речевой информации через ТА в режиме ожидания вызова (РА0019301 ТУ)	Техническое	ТОО "РЕНОМ"	103030, Москва, ул.Новослободская, д. 10 т.(095)430-9225
24	25.12.95 N 28	до 31.12.98	"Сизам"	Система защиты информации от НСД в ЛВС - по классу защищенности 1Д (ЛВС) и 6 классу защищенности для СВТ	Программное	НПФ "Кристалл	440017, Пенза, ул. Красная, 40 т(814-2)62-8131
25	11.01.96 N 29	до 31.12.98		Персональные ЭВМ типа PC/AT 486DX	Техническое	АОЗТ "ДОС" и АОЗТ "Стинс Коман"	141700, Московская обл., г.Долгопрудный ул.Летная,д.1. т.576-25-72
26	18.01.95 N 30	до 18.01.98	DALLAS LOCK 3.1	Программно-аппаратный комплекс защиты от НСД и обработки конфиденциальной информации DALLAS LOCK 3.1	Программно-аппаратное	Ассоциация защиты информации "Конфидент"	193060, г.Санкт-Петербург, ул.Пролетарской диктатуры, д.2. т.(812)278-1392
27	18.01.96 N 31	до 31.01.99	SECRET NET 1.10	Система защиты локальной вычислительной сети "SECRET NET", версия 1.10 (включая ее локальную версию) — по 6 классу защищенности для СВТ	Программно-аппаратное	АОЗТ "Информ-защита"	125438,г.Москва, Олимпийский пр., д.30. т.154-1368

МАТЕРИАЛ НОМЕРА

Руководство по информационной безопасности предприятия

(Site Security Handbook, RFC 1244)

P. Holbrook, J. Reynolds (редакторы)*

Содержание

Статус документа

Данное Руководство является продуктом деятельности рабочей группы по политике информационной безопасности предприятий (SSPHWG), в которую вошли представители групп безопасности и пользовательских сервисов движения IETF (Internet Engineering Task Force). Руководство содержит информацию для сообщества Интернет, оно не является стандартом, его распространение не ограничено.

Авторы

Ниже приведен список авторов Руководства по информационной безопасности. Без их труда появление Руководства было бы невозможным.

Dave Curry (Purdue University), Sean Kirkpatrick (Unisys), Tom Longstaff (LLNL), Greg Hollingsworth (Johns Hopkins University), Jeffrey Carpenter (University of Pittsburgh), Barbara Fraser (CERT), Fred Ostapik (SRI NISC), Allen Sturtevant (LLNL), Dan Long (BBN), Jim Duncan (Pennsylvania State University), Frank Byrum (DEC).

Предисловие редакторов

RFC 1244 – первая попытка снабдить пользователей ориентирами в области безопасной работы в Интернет. Как таковой, документ обречен на неполноту. К очевидным пробелам можно отнести ориентацию преимущественно на ресурсы безопасности, доступные в США. Мы будем признательны, если читатели, в соответствии с духом Интернет, пришлют нам замечания и дополнения. Особенно ценными были бы отзывы тех, кто применил Руководство на практике для выработки собственной политики безопасности и соответствующих процедур.

Руководство задумано как отправная точка будущих исследований. К нему разумно относиться как к полезному ресурсу, но не как к истине в последней инстанции. У каждой организации свои правила и возможности. Консультации со знающими людьми и, в частности, с юристами, помогут Вам восполнить пробелы данного Руководства.

1. Введение

1.1. Цель работы

Данное Руководство призвано помочь в выработке политики безопасности и соответствующих процедур для организаций, имеющих выход в Интер-

*Перевод с сокращениями

нет. В Руководстве перечисляются вопросы и факторы, которые следует проанализировать при формировании собственной политики безопасности предприятия. Даются некоторые рекомендации, обсуждается ряд смежных тем.

Руководство содержит лишь основные элементы, необходимые для выработки политики и процедур безопасности. Чтобы получить эффективный набор защитных средств, ответственным лицам придется принять много решений, заключить многочисленные соглашения, после чего настанет черед доведения политики безопасности до сотрудников и ее реализации.

1.2. На кого рассчитана работа

Данная работа рассчитана на руководителей и системных администраторов. Она не предназначается для программистов и разработчиков защищенных программ и систем. Основной упор делается на политику и процедуры, необходимые для поддержки технических средств, выбранных организацией.

В первую очередь Руководство предназначено для организаций, подключенных к Интернет. В то же время мы надеемся, что оно будет полезным для всех предприятий, имеющих сетевые контакты любого рода. Как введение в политику безопасности, данный документ поможет и организациям с изолированными компьютерными системами.

1.3. Определения

В Руководстве слова "организация" и "предприятие" трактуются как синонимы, обозначающие собственника компьютеров и иных сетевых ресурсов. В число сетевых ресурсов входят хосты, на которых работают пользователи, а также маршрутизаторы, терминальные серверы, ПК и другие устройства, имеющие связь с Интернет. Организация может быть конечным пользователем сервисов Интернет или поставщиком соответствующих услуг. Тем не менее, Руководство в основном рассчитано на конечных пользователей.

Предполагается, что организация может вырабатывать собственные политику и процедуры безопасности при согласии и поддержке реальных владельцев ресурсов.

Интернет — это совокупность сетей и машин, использующих семейство протоколов TCP/IP, соединенных шлюзами и разделяющих общие пространства имен и адресов [1].

Термин "системный администратор" относится ко всем тем, кто отвечает за повседневную работу ресурсов. Администрирование может выполнять группа людей или независимая компания.

Понятие "руководитель" обозначает сотрудника организации, вырабатывающего или одобряющего политику безопасности. Часто (но не всегда) руководитель одновременно является собственником ресурсов.

1.4. Близкие работы

Рабочая группа IETF по политике безопасности (Security Policy Working Group, SPWG) стремится выработать рекомендации для политики безопасности в рамках Интернет [23]. Эти рекомендации могут быть одобрены владельцами региональных сетей или иных ресурсов. Данное Руководство, возможно, окажется полезным инструментом реализации предлагаемой политики. Тем не менее, для обеспечения безопасности мало реализовать рекомендуемую политику, поскольку она затрагивает лишь сетевые аспекты и ничего не говорит о локальной защите.

1.5. Контекст

Данный документ отвечает на вопросы о том, что входит в политику безопасности, какие процедуры необходимы для обеспечения безопасности, что нужно делать в ситуациях, угрожающих безопасности. При выработке политики следует помнить не только о защите локальной сети, но также о нуждах и требованиях других подсоединенных сетей.

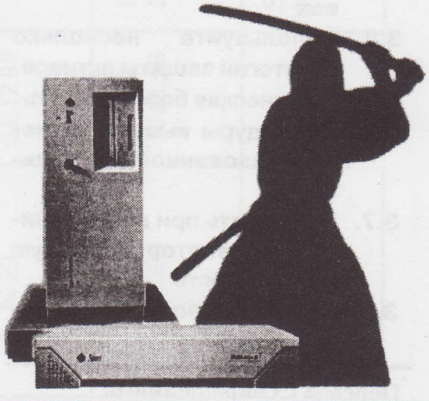
Руководство не является собранием рецептов по информационной безопасности. У каждой организации свои нужды; разница между корпорацией и академическим институтом весьма значительна. В то же время план защитных мероприятий, чтобы быть реальным, должен соответствовать потребностям и традициям конкретной организации.

В Руководстве не рассматриваются детали оценки рисков, планирования аварийных мероприятий, физической безопасности. Эти вещи необходимы для выработки и проведения в жизнь эффективной политики безопасности, но мы полагаемся в упомянутых вопросах на другие документы. Нами будут даны лишь общие указания.

Вопросы проектирования и реализации защищенных систем или программ также не будут нами рассматриваться.

1.6. Зачем нужны политика безопасности и процедуры безопасности?

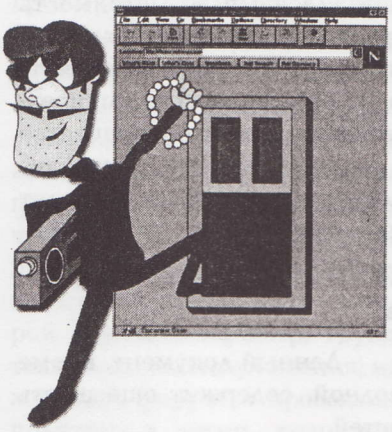
Как правило, интерес к информационной безопасности пропорционален имеющемуся в организации ощущению таящихся вокруг рисков и угроз.



За последние двадцать пять лет компьютерный мир претерпел радикальные изменения. Тогда, двадцать пять лет назад, большинство компьютеров находилось в ведении вычислительных центров. Они содержались в запертых помещениях, а обслуживающий персонал отвечал за тщательность администрирования и физическую безопасность. Связи с внешним миром были явлением редким. Редко возникали и угрозы информационной безопасности, исходившие в подавляющем большинстве случаев от штатных сотрудников. Угрозы состояли в неправильном использовании полномочий со стороны авторизованных пользователей, в подделке электронных документов, в вандализме и т.п. Для предотвращения подобных угроз было вполне достаточно стандартных мер: замков на дверях и учета использования всех ресурсов.

Вычислительная среда 1990-х совершенно иная. Многие системы размещены в частных офисах и небольших лабораториях и администрируются людьми, не состоящими в штате данной организации. Немало компьютеров подключено к Интернет; тем самым они оказываются связанными со всем миром, от Австралии до Америки.

Изменились и угрозы безопасности. Традиционный совет гласит: "Не записывайте пароли на листке и не кладите этот листок в стол, где его может кто-нибудь найти". С общемировыми связями через Интернет, злоумышленник, находящийся на противоположной стороне Земли, может среди ночи проникнуть в Вашу систему и выкрасть пароль, несмотря на то, что здание Вашей организации закрыто на все замки. Вирусы и черви могут передаваться от машины к машине. По Интернет'у могут разгуливать "электронные воры", высматривающие незакрытые окна и двери. Теперь злоумышленник может за несколько часов проверить наличие слабых мест в защите сотен компьютеров.



Системные администраторы и руководители должны знать современные угрозы, связанные с ними риски, размер возможного ущерба, а также набор доступных мер для предотвращения и отражения нападений.

В качестве иллюстрации некоторых проблем, связанных с информационной безопасностью, рассмотрим, вслед за [2], следующие сценарии. (Их автор — Russell Brand, которому мы выражаем признательность.)

- Системный программист получает сообщение о том, что главный подпольный бюллетень крэкеров распространяется с административной машины, находящейся в его ведении, и попадает в пять тысяч американских и западноевропейских компьютеров.

Спустя восемь недель тот же программист получил официальное уведомление, что информация из одного бюллетеня была использована для выведения из строя на пять часов службы "911" в одном большом городе.

- Пользователь звонит и сообщает, что он не может войти в систему под своим именем в 3 часа утра субботы. Администратор также не смог войти в систему. После перезагрузки и входа в однопользовательский режим он обнаруживает, что файл паролей пуст. К утру понедельника выясняется, что между данной машиной и местным университетом в привилегированном режиме было передано несколько файлов.

Во вторник утром на университетском компьютере была найдена копия стертого файла паролей вместе с аналогичными файлами с дюжины других машин.

Спустя неделю программист обнаруживает, что файлы инициализации системы изменены враждебным образом.

- Программист получает сообщение о том, что в компьютер правительственной лаборатории было совершено вторжение с подведомственной ему машины. Программисту предлагают предоставить регистрационную информацию для отслеживания нападавшего.

Спустя неделю программист получает список подведомственных компьютеров, подвергшихся успешным атакам крэкеров.

- Программисту звонит репортер и интересуется подробностями проникновения на компьютеры организации. Программист отвечает, что ничего не слышал о таких проникновениях.

Через три дня выясняется, что случай проникновения имел-таки место. Глава организации использовал в качестве пароля имя жены.

- Обнаруживаются модификации системных бинарных файлов.

После восстановления файлы в тот же день вновь оказываются модифицированными. Так повторяется несколько недель.

С подобными проблемами может столкнуться любая организация, имеющая выход в Интернет. Вы должны иметь заранее заготовленные ответы по крайней мере на следующие вопросы:

- Если Вы обнаруживаете в своей системе присутствие

злоумышленника, должны ли Вы оставить систему открытой и попытаться проследить за ним, или компьютер следует немедленно выключить и залатать обнаруженные дыры?

- Если злоумышленник использует компьютеры Вашей организации, должны ли Вы обращаться в правоохранительные органы? Кто принимает решение об обращении в органы? Если представитель властей предложит оставить системы открытыми, кто ответит за это решение?
- Какие шаги следует предпринять, если Вам звонят из другой организации и сообщают о подозрительных действиях со стороны одного из Ваших пользователей? Что, если этим пользователем оказывается местный системный администратор?

1.7. Основы подхода

Формирование политики и процедур безопасности на самом деле означает выработку плана действий по информационной защите. Один из возможных подходов к решению данной задачи предложил Fites с коллегами (см. [3]):

- Выясните, что Вы собираетесь защищать.
- Выясните, от чего Вы собираетесь защищаться.
- Определите вероятность угроз.
- Реализуйте меры, которые позволят защитить Ваши активы экономически оправданным образом.
- Постоянно возвращайтесь к предыдущим этапам и улучшайте защиту после выявления новых уязвимых мест.

В настоящем Руководстве основной упор делается на два последних этапа, однако следует помнить и о критической важности первых трех этапов для принятия эффективных решений в области безопасности. Давно известна истина, гласящая, что стоимость защиты не должна превосходить ущерб от осуществления угрозы. Без реалистичного представления о том, что защищается и каковы вероятные угрозы, следовать старому совету будет очень трудно.

1.8. Структура Руководства

Данный документ, кроме вводной, содержит еще шесть частей.

По форме каждая часть представляет собой обсуждение вопросов, которые организация должна рассмотреть при выработке политики безопасности и формировании процедур, реализующих эту политику. В некоторых случаях анализируются имеющиеся альтернативы и аргументы в пользу выбора какой-либо из них. Мы старались по возможности избегать диктата, поскольку многое зависит от местных условий. Не все из рассматриваемых вопросов важны для всех организаций, но организации должны хотя бы бегло ознакомиться с каждым из них, чтобы не упустить ничего существенного.

В плане общей структуры обсуждение политики безопасности предшествует рассмотрению процедур, реализующих политику.

Раздел 2 посвящен выработке официальной политики предприятия, касающейся доступа к вычислительным ресурсам. Рассматриваются также вопросы нарушения политики. Политика определяет набор необходимых процедур, поэтому руководителю следует сначала определиться по политическим вопросам, и только после этого переходить к процедурным. Ключевым компонентом формирования политики безопасности является производимая в той или иной форме оценка рисков, позволяющая определить, что необходимо защищать и каков объем ресурсов, которые разумно выделить на защиту.

Когда политика выработана, можно приступать к созданию процедур, решающих проблемы безопасности. В разделе 3 определяются и предлагаются действия, которые необходимо предпринять при возникновении подозрений по поводу совершения неавторизованных операций. Анализируются также ресурсы, необходимые для предотвращения нарушений режима безопасности.

В разделе 4 перечисляются типы процедур, служащих для предотвращения нападений. Профилактика — основа безопасности. По данным группы реагирования на нарушения безопасности и ее координационного центра (Computer Emergency Response Team/Coordination Center, CERT/CC), не менее 80% инцидентов, которые им довелось наблюдать, объяснялись плохим выбором паролей.

Раздел 5 посвящен реагированию на нарушения безопасности, то есть кругу вопросов, с которыми организация сталкивается, когда кто-то отступает от политики безопасности. Когда такое случается, приходится принимать целый комплекс решений, но многие из них можно продумать заранее. По крайней мере, следует договориться о распределении обязанностей и способах взаимодействия. И здесь определяющую роль играет политика безопасности, рассматриваемая в разделе 2.

Тема раздела 6 — меры, предпринимаемые после ликвидации нарушения безопасности. Планирование защитных действий — это непрерывный циклический процесс. Очередной инцидент — прекрасный повод для пересмотра и улучшения политики и процедур.

Завершает Руководство список литературы.

2. Выработка официальной политики предприятия в области информационной безопасности

2.1. Краткий обзор

2.1.1. Организационные вопросы

Целью разработки официальной политики предприятия в области информационной безопасности является определение правильного (с точки зрения организации) способа использования вычислительных и коммуникационных ресурсов, а также разработка процедур, предотвращающих или реагирующих на нарушения режима безопасности. Чтобы достичь данной цели, следует учесть специфику конкретной организации.

Во-первых, необходимо принять во внимание цели и основные направления деятельности организации. Например, на военной базе и в университете существенно разные требования к конфиденциальности.

Во-вторых, разрабатываемая политика должна согласовываться с существующими законами и правилами, относящимися к организации. Значит, эти законы и правила необходимо выявить и принять во внимание при разработке политики.

В-третьих, если локальная сеть организации не является изолированной, вопросы безопасности следует рассматривать в более широком контексте. Политика должна освещать проблемы, возникающие на локальном компьютере из-за действий удаленной стороны, а также удаленные проблемы, причиной которых является локальный хост или пользователь.

2.1.2. Кто делает политику?

Политика безопасности должна стать результатом совместной деятельности технического персонала, способного понять все аспекты политики и ее реализации, а также руководителей, способных влиять на проведение политики в жизнь. Нереализуемая или неподдерживаемая политика бесполезна.

Поскольку политика безопасности так или иначе затрагивает всех сотрудников организации, следует позаботиться о том, чтобы у Вас было достаточно полномочий для принятия политических решений. Хотя некоторой группе (например, группе технического обслуживания) может быть поручено проведение политики в жизнь, возможно, нужна группа более высокого ранга для поддержки и одобрения политики.

2.1.3. Кого затрагивает политика?

Политика безопасности потенциально затрагивает всех пользователей компьютеров в организации, причем по нескольким аспектам. Пользователи могут отвечать за администрирование собственных паролей. Системные администраторы обязаны ликвидировать слабые места в защите и надзирать за работой всех систем.

Важно с самого начала работы над политикой безопасности правильно подобрать состав коллектива разработчиков. Возможно, на предприятии уже есть группа информационной безопасности; естественно, люди из этой группы считают безопасность своей вотчиной. Следует привлечь также специалистов по аудиту и управлению, по физической безопасности, по информационным системам и т.п. Тем самым будет подготовлена почва для одобрения политики.

2.1.4. Распределение ответственности

Ключевым элементом политики является доведение до каждого его обязанностей по поддержанию режима безопасности. Политика не может предусмотреть всего, однако она обязана гарантировать, что для каждого вида проблем существует ответственный.

В связи с информационной безопасностью можно выделить несколько уровней ответственности. На первом уровне каждый пользователь компьютерного ресурса обязан заботиться о защите своего счета. Пользователь, допустивший компрометацию своего счета, увеличивает вероятность компрометации других счетов и ресурсов.

Системные администраторы образуют другой уровень ответственности. Они должны обеспечивать защиту компьютерных систем. Сетевых администраторов можно отнести к еще более высокому уровню.

2.2. Оценка рисков

2.2.1. Общие положения

Один из главных побудительных мотивов выработки политики безопасности состоит в получении уверенности, что деятельность по защите информации построена экономически оправданным образом. Данное положение кажется очевидным, но, вообще говоря, возможны ситуации, когда усилия прикладываются не там, где нужно. Например, много говорят и пишут о хакерах; в то же время в большинстве обзоров по информационной безопасности утверждается, что в типичной организации ущерб от внутренних, "штатных" злоумышленников значительно больше.

Процесс анализа рисков включает в себя определение того, что следует защищать, от чего защищать и как это делать. Необходимо рассмотреть все возможные риски и ранжировать их в зависимости от потенциального размера ущерба. Этот процесс состоит из множества экономических решений. Давно замечено, что затраты на защиту не должны превышать стоимости защищаемого объекта.

Полное рассмотрение проблемы анализа рисков выходит за пределы данной публикации. Интересующимся мы рекомендуем обратиться к работам [3] и [16]. Тем не менее, в следующих пунктах будут затронуты два этапа процесса анализа рисков:

- идентификация активов,
- идентификация угроз.

Главной целью деятельности в области информационной безопасности является обеспечение доступности, конфиденциальности и целостности каждого актива. При анализе угроз следует принимать во внимание их воздействие на активы по трем названным направлениям.

2.2.2. Идентификация активов

Один из этапов анализа рисков состоит в идентификации всех объектов, нуждающихся в защите. Некоторые активы (например, аппаратура) идентифицируются очевидным образом. Про другие (например, про людей, использующих информационные системы) нередко забывают. Необходимо принять во внимание все, что может пострадать от нарушений режима безопасности.

В свое время Pfleeger [16] предложил следующую классификацию активов:

- Аппаратура: процессоры, модули, клавиатуры, терминалы, рабочие станции, персональные компьютеры, принтеры, дисководы, коммуникационные линии, терминальные серверы, маршрутизаторы.
- Программное обеспечение: исходные тексты, объектные модули, утилиты, диагностические программы, операционные системы, коммуникационные программы.
- Данные: обрабатываемые, непосредственно доступные, архивированные, сохраненные в виде резервной копии, регистрационные журналы, базы данных, передаваемые по коммуникационным линиям.
- Люди: пользователи, обслуживающий персонал.
- Документация: по программам, по аппаратуре, системная, по административным процедурам.
- Расходные материалы: бумага, формы, красящая лента, магнитные носители.

2.2.3. Идентификация угроз

После того, как выявлены активы, нуждающиеся в защите, необходимо идентифицировать угрозы этим активам и размеры возможного ущерба. Это поможет понять, каких угроз следует опасаться больше всего.

В следующих пунктах перечисляются некоторые из возможных угроз.

2.2.3.1. Несанкционированный доступ

Несанкционированный доступ к компьютерным ресурсам — угроза, типичная для большинства организаций. Несанкционированный доступ может принимать различные формы. Иногда это нелегальное использование счета другого пользователя для получения доступа к системе. В других случаях ресурсами пользуются без предварительно полученного разрешения.

Степень важности проблемы несанкционированного доступа для разных организаций разная. Порой передача прав доступа неавторизованному пользователю может привести к разрушению магнитных носителей. Чаще несанкционированный доступ облегчает исполнение других угроз. Разнится и вероятность нападения: некоторые организации (известные университеты, правительственные и военные учреждения) как бы притягивают к себе злоумышленников. Следовательно, риск несанкционированного доступа меняется от предприятия к предприятию.

2.2.3.2. Нелегальное ознакомление с информацией

Нелегальное ознакомление с информацией — другая распространенная угроза. Определите степень конфиденциальности информации, хранящейся в Ваших компьютерах. Расшифровка файла паролей откроет дорогу несанкционированному доступу. Мимолетный взгляд на Ваше коммерческое предложение может дать конкуренту решающее преимущество. Техническая статья способна вместить в себя годы напряженных исследований.

2.2.3.3. Отказ в обслуживании

Компьютеры и сети предоставляют своим пользователям множество ценных услуг, от которых зависит эффективная работа многих людей. Когда услуги вдруг становятся недоступными, страдает производительность труда.

Отказ в обслуживании возникает по разным причинам и проявляется по-разному. Сеть может прийти в неработоспособное состояние от поддельного пакета, от перегрузки или по причине отказа компонента. Вирус способен замедлить или парализовать работу компьютерной системы. Каждая организация должна определить для себя набор необходимых сервисов и для каждого из них проанализировать последствия его недоступности.

2.3. Политические вопросы

При разработке политики безопасности необходимо дать ответы на ряд вопросов, а именно:

- Кто имеет право использовать ресурсы?
- Как правильно использовать ресурсы?
- Кто наделен правом давать привилегии и разрешать использование?
- Кто может иметь административные привилегии?
- Каковы права и обязанности пользователей?
- Каковы права и обязанности системных администраторов по отношению к обычным пользователям?
- Как работать с конфиденциальной информацией?

Ниже мы обсудим эти вопросы. Кроме того, возможно, Вы захотите отразить в политике этические аспекты использования вычислительных ресурсов. В таком случае Вам помогут работы [17] и [18].

2.3.1. Кто имеет право использовать ресурсы?

Одним из шагов в разработке политики безопасности является определение того, кто может использовать Ваши системы и сервисы. Должно быть явно сказано, кому дается право использовать те или иные ресурсы.

2.3.2. Как правильно использовать ресурсы?

После определения круга лиц, имеющих доступ к системным ресурсам, необходимо описать правильные и неправильные способы использования ресурсов. Для разных категорий пользователей (студентов, внешних пользователей, штатных сотрудников и т.д.) эти способы могут различаться. Должно быть явно сказано, что допустимо, а что — нет. Могут быть описаны также ограничения на использование определенных ресурсов. При этом Вам придется специфицировать уровни доступа разных групп пользователей.

Пользователи должны знать, что они несут ответственность за свои действия независимо от применяемых защитных средств и что использовать чужие счета и обходить механизмы безопасности запрещено.

Для регламентации доступа к ресурсам нужно дать ответы на следующие вопросы:

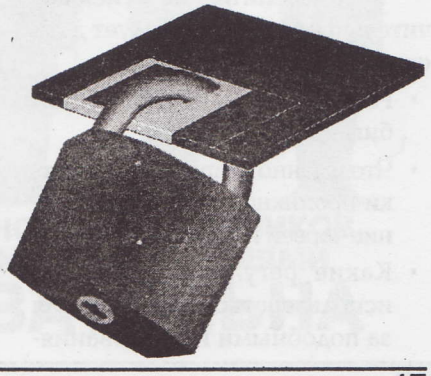
- Разрешается ли использование чужих счетов?
- Разрешается ли отгадывать чужие пароли?
- Разрешается ли разрушать сервисы?
- Должны ли пользователи предполагать, что если файл доступен всем на чтение, то они имеют право его читать?
- Имеют ли право пользователи модифицировать чужие файлы, если по каким-либо причинам у них есть доступ на запись?
- Должны ли пользователи разделять счета?

В большинстве случаев ответы на подобные вопросы будут отрицательными.

В политике могут найти отражение авторские и лицензионные права на программное обеспечение. Лицензионное соглашение с поставщиком налагает на организацию определенные обязательства; чтобы не нарушить их, необходимо приложить некоторые усилия. Кроме того, Вы, возможно, захотите проинформировать пользователей, что присваивать защищенное авторскими правами программное обеспечение запрещено законом.

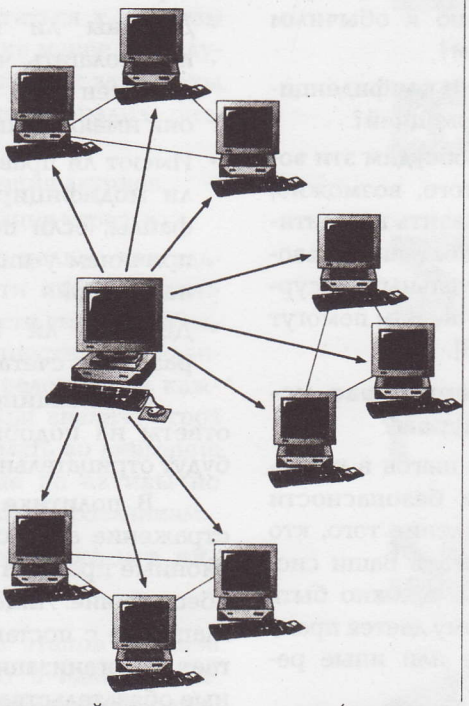
Более точно, Вы должны довести до сведения пользователей, что:

- Копировать авторское и лицензионное программное обеспечение запрещено, за исключением явно оговоренных случаев.
- Они всегда могут узнать авторский/лицензионный статус программного обеспечения.

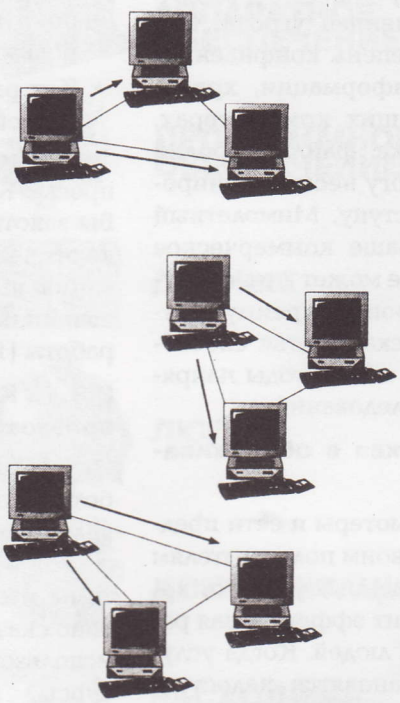


Распределение прав доступа:

централизованное:



децентрализованное:



- В случае сомнений копировать не следует.

Политика в области правильного использования ресурсов очень важна. Если явно не сказано, что запрещено, Вы не сможете доказать, что пользователь нарушил политику безопасности.

Бывают исключительные случаи, когда в исследовательских целях пользователи или администраторы пытаются "расколоть" защиту сервиса или лицензионной программы. Политика должна давать ответ на вопрос, разрешены ли подобные исследования в Вашей организации и каковы могут быть их рамки.

Применительно к исключительным случаям следует дать ответы на такие вопросы:

- Разрешены ли вообще подобные исследования?
- Что именно разрешено: попытки проникновения, выращивание червей и вирусов и т.п.?
- Какие регуляторы должны использоваться для контроля за подобными исследованиями (например, их изоляция в рамках отдельного сегмента сети)?
- Как защищены пользователи (в том числе внешние) от подобных исследований?
- Как получать разрешение на проведение исследований?

В случае, когда получено разрешение на исследование, следует изолировать тестируемые сегменты от основной сети предприятия. Черви и вирусы не должны выпускаться в "живую" сеть.

Возможно, Вы захотите заключить контракт с отдельными людьми или сторонней организацией на предмет проверки защищенности Ваших сервисов. Частью проверки могут стать попытки взлома систем. Это также должно найти отражение в политике Вашего предприятия.

2.3.3. Кто наделен правом давать привилегии и разрешать использование?

Политика безопасности должна давать ответ на вопрос, кто распоряжается правами доступа к сервисам. Кроме того, необходимо точно знать, какие именно права им позволено распределять. Если Вы не управляете процессом наделения правами доступа к Вашей системе, Вы не контролируете и круг пользователей. Если Вы знаете, кто отвечает за распределение прав, Вы всегда сможете узнать, давались ли определенные права конкретному пользователю, или он получил их нелегально.

Существует много возможных схем управления распределением прав доступа к сервисам. При выборе подходящей целесообразно принять во внимание следующие моменты:

- Будут ли права доступа распределяться централизованно или из нескольких мест?

Можно установить единый распределительный пункт или передать соответствующие права подразделениям и отделам. Все зависит от того, какое соотношение между безопасностью и удобством Вы считаете допустимым. Чем сильнее централизация, тем проще поддерживать режим безопасности.

- Какие методы предполагается использовать для заведения счетов и запрещения доступа?

Вы должны проверить механизм заведения счетов с точки зрения безопасности. В наименее ограничительном режиме уполномоченные лица непосредственно входят в систему и заводят счета вручную или с помощью утилит. Обычно подобные утилиты предполагают высокую степень доверия к использующим их лицам, которые получают значительные полномочия. Если Вы останавливаете свой выбор на таком режиме, Вам необходимо найти достаточно надежного человека. Другой крайностью является применение интегрированной системы, которую запускают уполномоченные лица или даже сами пользователи. В любом случае, однако, остается возможность злоупотреблений.

Следует разработать и тщательно документировать специальные процедуры заведения новых счетов, чтобы избежать недоразумений и уменьшить число ошибок. Нарушение безопасности при заведении счетов возможно не только по злому умыслу, но и в результате ошибок. Наличие ясных и хорошо документированных процедур внушает уверенность, что подобные ошибки не случатся. Кроме того, необходимо удостовериться, что люди, исполняющие процедуры, понимают их.

Наделение пользователей правами доступа — одна из самых уязвимых процедур. Прежде всего, следует позаботиться, чтобы начальный пароль не был легко угадываемым. Целесообразно избегать использования начальных паролей, являющихся функцией от имени пользователя или его полного имени. Не стоит автоматически генерировать начальные пароли, если результат генерации легко предсказуем. Далее, нельзя разрешать пользователям до бесконечности полагаться на начальный пароль. По возможности следует принуждать пользователей менять начальный пароль при первом входе в систему. Правда, даже такая мера бессильна против людей, которые вообще не пользуются своим счетом, сохраняя до бесконечности уязвимый начальный пароль. В некоторых организациях неиспользуемые счета уничтожают, заставляя их владельцев повторно проходить процедуру регистрации.

2.3.4. Кто может иметь административные привилегии?

Одно из решений, которое должно быть тщательно взвешено, относится к выбору лиц, имеющих доступ к административным привилегиям и паролям для Ваших сервисов. Очевидно, подобный доступ должны иметь системные администраторы, но неизбежны ситуации, когда за привилегиями будут обращаться другие пользователи, что следует с самого начала предусмотреть в политике безопасности. Ограничение прав — один из способов защититься от угроз со стороны своих пользователей. Необходим, однако, сбалансированный подход, когда ограничение прав не мешает людям делать свое дело. Разумнее всего давать пользователям ровно те права, которые нужны им для выполнения своих обязанностей.

Далее, сотрудники, имеющие специальные привилегии, должны быть подотчетны некоторому должностному лицу, и это также необходимо отразить в политике безопасности предприятия. Если "привилегированные" люди перестают быть подотчетными, Вы рискуете потерять контроль над своей системой и лишиться возможности расследовать случаи нарушения режима безопасности.

2.3.5. Каковы права и обязанности пользователей?

Политика безопасности должна содержать положения о правах и обязанностях пользователей применительно к использованию компьютерных систем и сервисов предприятия. Должно быть явно оговорено, что пользователи обязаны понимать и выполнять правила безопасной эксплуатации систем. Ниже приведен перечень тем, которые целесообразно осветить в данном разделе политики безопасности:

- Каковы общие рамки использования ресурсов? Существуют ли ограничения на ресурсы и каковы они?
- Что является злоупотреблением с точки зрения производительности системы?
- Разрешается ли пользователям совместное использование счетов?
- Как "секретные" пользователи должны охранять свои пароли?

- Как часто пользователи должны менять пароли? Каковы другие аналогичные ограничения и требования?
- Как обеспечивается резервное копирование — централизованно или индивидуально?
- Как реагировать на случаи просмотра конфиденциальной информации?
- Как соблюдается конфиденциальность почты?
- Какова политика в отношении неправильно адресованной почты или отправлений по спискам рассылки или в адрес дискуссионных групп (непристойности, приставания и т.п.)?
- Какова политика по вопросам электронных коммуникаций (подделка почты и т.п.)?

Ассоциация электронной почты (The Electronic Mail Association, EMA) подготовила статью о конфиденциальности электронной почты в организациях [4]. Основное положение статьи состоит в том, что каждая организация должна разработать политику защиты права сотрудников на тайну. Рекомендуется, чтобы эта политика охватывала все возможные среды, а не только электронную почту.

Предлагается пять критериев оценки подобной политики:

- Согласуется ли политика с существующим законодательством и с обязанностями по отношению к третьим сторонам?
- Не ущемляются ли без нужды интересы работников, работодателей или третьих сторон?
- Реалистична ли политика и вероятно ли ее проведение в жизнь?
- Затрагивает ли политика все виды передачи и хранения информации, используемые в организации?
- Объявлена ли политика заранее и получила ли она одобрение всех заинтересованных сторон?

2.3.6. Каковы права и обязанности системных администраторов по отношению к обычным пользователям?

Должен соблюдаться баланс между правом пользователей на тайну и обязанностью системного администратора собирать достаточно информации для разрешения проблем и расследования случаев нарушения режима безопасности. Политика должна определять границы, в пределах которых системный администратор вправе исследовать пользовательские файлы с целью разрешения проблем и для иных нужд, и каковы права пользователей. Можно также сформулировать положение относительно обязанности администраторов соблюдать конфиденциальность информации, полученной при оговоренных выше обстоятельствах. Политика должна содержать ответы на несколько вопросов:

- Может ли администратор отслеживать или читать пользовательские файлы при каких-либо обстоятельствах?
- Какие обязательства администратор при этом берет на себя?
- Имеют ли право сетевые администраторы исследовать сетевой трафик?

2.3.7. Как работать с конфиденциальной информацией?

Прежде чем предоставлять пользователям доступ к Вашим сервисам, следует определить, каков уровень защиты данных на Вашей системе. Тем самым Вы сможете определить уровень конфиденциальности информации, которую пользователи могут у Вас размещать. Наверное, Вы не хотите, чтобы пользователи хранили секретные сведения на компьютерах, которые Вы не собираетесь как

следует защищать. Следует сообщить пользователям, какие сервисы (при наличии таковых) пригодны для хранения конфиденциальной информации. Должны рассматриваться различные способы хранения данных (на диске, ленте, файловом сервере и т.д.). Этот аспект политики должен быть согласован с правами системных администраторов по отношению к обычным пользователям (см. предыдущий пункт).

2.4. Что делать, когда политику безопасности нарушают

Очевидно, что любая официальная политика, вне зависимости от ее отношения к информационной безопасности, время от времени нарушается. Нарушение может явиться следствием пользовательской небрежности, случайной ошибки, отсутствия должной информации о текущей политике или ее непонимания. Возможно также, что некое лицо или группа лиц сознательно совершают действия, прямо противоречащие утвержденной политике безопасности.

Необходимо заранее определить характер действий, предпринимаемых в случае обнаружения нарушений политики, чтобы эти действия были быстрыми и правильными. Следует организовать расследование, чтобы понять, как и почему нарушение стало возможным. После этого нужно внести коррективы

в систему защиты. Тип и серьезность корректив зависят от типа случившегося нарушения.

2.4.1. Выработка ответа на нарушение политики

Политику безопасности могут нарушать самые разные лица. Некоторые из них являются своими, местными пользователями, другие нападают извне. Полезно определить сами понятия "свои" и "чужие", исходя из административных, правовых или политических положений. Эти положения очерчивают характер санкций, которые можно применить к нарушителю — от письменного выговора до привлечения к суду. Таким образом, последовательность ответных действий зависит не только от типа нарушения, но и от вида нарушителя; она должна быть продумана задолго до первого инцидента, хотя это и непросто.

Следует помнить, что правильно организованное обучение — лучшая защита. Вы обязаны поставить дело так, чтобы не только внутренние, но и внешние легальные пользователи знали положения Вашей политики безопасности. Если Вы будете располагать свидетельством подобного знания, это поможет Вам в будущих правовых акциях, когда таковые понадобятся.

Проблемы с нелегальными пользователями в общем те же. Нужно получить ответы на вопросы о том, какие типы пользователей нарушают политику, как и зачем они это делают. В зависимости от результатов расследования Вы можете просто заткнуть дыру в защите и удовлетвориться полученным уроком или предпочтете более крутые меры.

2.4.2. Что делать, когда местные пользователи нарушают политику безопасности сторонней организации

Каждое предприятие должно заранее определить набор административных санкций, применяемых к местным пользователям, нарушающим политику безопасности сторонней организации. Кроме того, необходимо позаботиться о защите от ответных действий сторонней организации. При выработке политики безопасности следует учесть все юридические положения, применимые к подобным ситуациям.

2.4.3. Спецификация контактов с внешними организациями и определение ответственных

Политика безопасности предприятия должна содержать процедуры для взаимодействия с внешними организациями, в число которых входят правоохранительные органы, другие организации, команды "быстрого реагирования" (CERT, CIAC), средства массовой информации. В процедурах должно быть определено, кто имеет право на такие контакты и как именно они совершаются. Среди прочих, нужно дать ответы на следующие вопросы:

- Кто может разговаривать с прессой?

- Когда следует обращаться в правоохранительные органы?
- Если соединение выполняется из сторонней организации, имеет ли право системный администратор обратиться в эту организацию?
- Какого рода сведения об инцидентах могут выходить за пределы организации?

Детальная информация по контактам должна быть постоянно доступна вместе с ясно определенными процедурами отработки этих контактов.

2.4.4. Каковы обязанности по отношению к соседям и другим пользователям Интернет?

Рабочая группа по политике безопасности (Security Policy Working Group, SPWG) сообщества Интернет опубликовала документ под названием "Основы политики для безопасной работы в Интернет" [23]. В нем Интернет трактуется как совместное предприятие, в котором пользователи должны помогать друг другу в поддержании режима безопасности. Это положение следует учитывать при разработке политики предприятия. Главный вопрос состоит в том, какой информацией можно делиться с соседями. Ответ зависит как от типа организации (военная, учебная, коммерческая и т.д.), так и от характера случившегося нарушения.

2.4.5. Процедурные вопросы реагирования на нарушения

Помимо политических положений, необходимо продумать и написать процедуры, исполняемые в случае обнаружения нарушений режима безопасности. Данный вопрос подробно рассматривается в следующей главе. Для всех видов нарушений должны быть заготовлены соответствующие процедуры.

2.5. Пресекать или следить?

Когда на организацию совершается нападение, грозящее нарушением информационной безопасности, стратегия ответных действий может строиться под влиянием двух противоположных подходов.

Если руководство опасается уязвимости предприятия, оно может предпочесть стратегию "защититься и продолжить". Главной целью подобно-

го подхода является защита информационных ресурсов и максимально быстрое восстановление нормальной работы пользователей. Действиям нарушителя оказывается максимальное противодействие, дальнейший доступ предотвращается, после чего немедленно начинается процесс оценки нанесенных повреждения и восстановления. Возможно, при этом придется выключить компьютерную систему, закрыть доступ в сеть или предпринять иные жесткие меры. Оборотная сторона данной медали состоит в том, что пока злоумышленник не выявлен, он может вновь напасть на эту же или другую организацию прежним или новым способом.

Другой подход, "выследить и осудить", опирается на иные философию и систему целей. Основная цель состоит в том, чтобы позволить злоумышленнику продолжать свои действия, пока организация не сможет установить его личность. Такой подход нравится правоохранительным органам. К сожалению, эти органы не смогут освободить организацию от ответственности, если пользователи обратятся в суд с иском по поводу ущерба, нанесенного их программам и данным.

Судебное преследование — не единственный возможный исход установления личности нарушителя. Если виновным оказался штатный сотрудник или студент, организация может предпочесть дисциплинарные меры. В политике безопасности должны быть перечислены допустимые варианты

наказания и критерии выбора одного или нескольких из них в зависимости от личности виновного.

Руководство организации должно заранее тщательно взвесить различные возможности при выборе стратегии ответных действий. В принципе стратегия может зависеть от конкретных обстоятельств нападения. Возможен и выбор единой стратегии на все случаи жизни. Нужно принять во внимание все за и против и проинформировать пользователей о принятом решении, чтобы они в любом случае осознавали степень своей уязвимости.

Следующий контрольный перечень помогает сделать выбор между стратегиями "защититься и продолжить" и "выследить и осудить".

При каких обстоятельствах предпочесть стратегию "защититься и продолжить":

1. Активы организации недостаточно защищены.
2. Продолжающееся вторжение сопряжено с большим финансовым риском.
3. Нет возможности или намерения осудить злоумышленника.
4. Неизвестен круг пользователей.
5. Пользователи неопытны, а их работа уязвима.
6. Пользователи могут привлечь организацию к суду за нанесенный ущерб.

При каких обстоятельствах предпочесть стратегию "выследить и осудить":

1. Активы и системы хорошо защищены.
2. Имеются хорошие резервные копии.
3. Угроза активам организации меньше потенциального ущерба от будущих повторных вторжений.
4. Имеет место согласованная атака, повторяющаяся с большой частотой и настойчивостью.
5. Организация притягивает злоумышленников и, следовательно, подвергается частым атакам.
6. Организация готова идти на риск, позволяя продолжить вторжение.
7. Действия злоумышленника можно контролировать.
8. Доступны развитые средства отслеживания, так что преследование нарушителя имеет шансы на успех.
9. Обслуживающий персонал обладает достаточной квалификацией для успешного выслеживания.
10. Руководство организации желает осудить злоумышленника.
11. Системный администратор знает, какого рода информация обеспечит успешное преследование.
12. Имеется тесный контакт с правоохранительными органами.
13. В организации есть человек, хорошо знающий соответствующие законы.
14. Организация готова к искам собственных пользователей по поводу программ и данных, скомпрометированных во время выслеживания злоумышленника.

2.6. Толкование политики безопасности

Важно определить, кто будет интерпретировать политику безопасности. Это может быть отдельное лицо или комитет. Вне зависимости от того, насколько хорошо она написана, политика безопасности время от времени нуждается в разъяснении, а заодно и в пересмотре.

2.7. Гласность политики безопасности

После того, как положения политики безопасности записаны и одобрены, необходимо начать активный процесс, гарантирующий, что политика вос-

принята и обсуждена. Почтовую рассылку нельзя признать достаточно мерой. Прежде чем политика вступит в силу, следует отвести время для дискуссий, чтобы все заинтересованные пользователи могли высказать свое мнение и указать на недостатки политики. В идеале политика должна соблюдать баланс между безопасностью и производительностью труда.

Целесообразно провести собрания, чтобы выслушать пожелания пользователей и заодно убедиться в правильном понимании ими предложенной политики. (Творцы политики порой бывают несколько косноязычны.) В собраниях должны участвовать все: от высшего руководства до младших специалистов. Безопасность — забота общая.

Помимо усилий по оглашению политики на начальном этапе, необходимо постоянно напоминать о ней. Опытные пользователи нуждаются в периодических напоминаниях, новичкам ее нужно разъяснять, вводя в курс дела. Прежде чем допускать сотрудника к работе, разумно получить его подпись под свидетельством о том, что он прочитал и понял политику безопасности. В ситуациях, чреватых судебным разбирательством после нарушения политики, бумага с подписью может оказаться весьма кстати.

3. Выработка процедур для предупреждения нарушений безопасности

Политика безопасности определяет, что нуждается в защите. В данной главе обсуждаются процедуры безопасности, специфицирующие, каким образом политика будет проводиться в жизнь.

3.1. Политика безопасности определяет, что следует защищать

Политика безопасности отвечает на вопрос ЧТО: что следует защищать, что является самым важным, что за свойства у защищаемых объектов, что за подход к проблемам безопасности избран.

Сама по себе политика безопасности не говорит, КАК защищаются объекты. Ответы на вопросы КАК дают процедуры безопасности, рассматриваемые в данной главе. Политика безопасности оформляется в виде высокоуровневого документа, описывающего общую стратегию. Процедуры безопасности должны в деталях специфицировать шаги, предпринимаемые организацией для собственной защиты.

Политика безопасности должна включать в себя общую оценку рисков по отношению к наиболее вероятным угрозам и оценку возможных последствий осуществления этих угроз (см. раздел 2.2). Частью процесса оценки рисков является составление списка активов, нуждающихся в защите (см. п. 2.2.2). Данная информация необходима для выработки экономически эффективных (практичных) процедур.

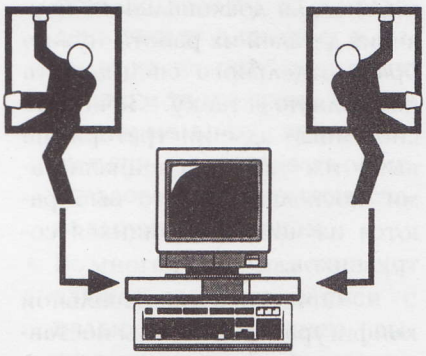
Заманчиво начать разработку процедур безопасности, отправляясь от защитных механизмов: "На всех компьютерах нашей организации должны вестись регистрационные журналы, модемы обязаны выполнять обратный дозвон, а всем пользователям необходимо выдать интеллектуальные карточки". Однако подобный подход может повести к массированной защите областей с небольшим риском и к недостаточной защите действительно уязвимых участков. Если же начать с политики и описанных ею рисков, можно быть уверенным, что процедуры обеспечивают достаточный уровень защиты для всех активов.

3.2. Выявляя возможные проблемы

Чтобы определить риски, необходимо выявить уязвимые места. Одна из целей политики безопасности состоит в том, чтобы прикрыть слабости и тем самым уменьшить риск для максимально возможного числа активов. В последующих пунктах представлены наиболее типичные слабости. Данный перечень ни в коей мере нельзя считать исчерпывающим. Кроме того, следует учитывать, что обычно у каждой организации находится несколько уникальных, присущих только ей уязвимых мест.

3.2.1. Точки доступа

Точки доступа обычно используются авторизованными пользователями для входя в систему. Наличие большого числа точек доступа увеличивает риск нелегального доступа к компьютерам организации и другим сетевым ресурсам.



Связь с внешними сетями открывает доступ к ресурсам организации всем лицам, подключенным к этим внешним сетям. Обычно сетевое соединение обеспечивает доступ к большому числу сервисов, каждый из которых может быть скомпрометирован.

Коммутируемые линии, в зависимости от конфигурации, могут дать доступ только к входному порту одной системы или ко всей сети, если они подключены к терминальному серверу.

Терминальные серверы сами по себе могут стать источником проблем, поскольку зачастую они лишены средств проверки подлинности пользователей. Нередко злоумышленники для сокрытия своих действий используют именно терминальные серверы, соединяясь с ними по местному телефону и уже через них выходя в локальную сеть. Некоторые терминальные серверы сконфигурированы таким образом, что к ним можно получить доступ по TELNET [19], находясь вне локальной сети, и затем выполнить TELNET во внешний мир, что существенно затрудняет отслеживание злоумышленников.

3.2.2. Неправильно сконфигурированные системы

Значительная часть "дыр" в защите приходится на неправильно сконфигурированные системы. Современные операционные системы и сопутствующее им программное обеспечение стали настолько сложными, что для досконального изучения деталей их работы нужно брать отдельного специалиста на полную ставку. Зачастую системные администраторы не являются такими специалистами, поскольку просто выбираются из числа имеющихся сотрудников.

Отчасти в неправильной конфигурации повинны поставщики, поскольку в целях упрощения процесса установки они выбирают начальные конфигурации, которые при определенных условиях не являются безопасными.

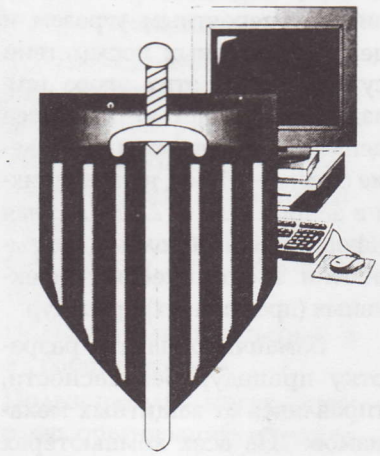
3.2.3. Программные ошибки

Программное обеспечение никогда не станет безошибочным. Обычным методом несанкционированного доступа является использование ошибок в защитных средствах. Частичным решением проблемы является получение информации об обнаружении подобных ошибок и внесение соответствующих исправлений в программы. Об ошибках необходимо сообщать поставщику, чтобы исправления вносились и распространялись централизованно.

3.2.4. Внутренние враги

Штатные сотрудники могут составлять значительную угрозу для информационной безопасности организации. Зачастую они имеют непосредственный доступ к аппаратным компонентам компьютеров и сетевых устройств. Наличие такого доступа облегчает компрометацию большинства систем. Так, в случае настольных рабочих станций, нетрудно получить привилегии суперпользователя. В случае локальной сети можно отслеживать всю передаваемую информацию, в том числе и конфиденциальную.

3.3. Выбор регуляторов для практичной защиты активов



После того, как выяснено, что нуждается в защите и оценены риски, грозящие активам, необходимо решить, как реализовать средства защиты. Регуляторы и защитные механизмы следует выбирать так, чтобы успешно и в то же время экономически эффективно противостоять угрозам, выявленным в процессе анализа рисков. Нет смысла тратить большие суммы денег и без нужды ограничивать доступ пользователей там, где риск нападения невелик.

3.3.1. Выбор подходящего набора регуляторов безопасности

Выбранные Вами регуляторы представляют собой реальное воплощение Вашей политики безопасности. Они образуют первую (и главную) линию обороны. В этой связи особенно важно, чтобы регуляторы в совокупности составляли правильный набор. Если наибольшую угрозу для Вашей системы составляют внешние злоумышленники, то, как правило, нет смысла использовать биометрические устройства для аутентификации обычных, внутренних пользователей. Если, с другой стороны, основная опасность состоит в неавторизованном использовании вычислительных ресурсов внутренними пользователями, Вы, вероятно, захотите воспользоваться очень строгими процедурами автоматического учета совершаемых действий.

3.3.2. Доверяйте здравому смыслу

Здравый смысл — лучшее средство формирования политики безопасности. Тщательная проработка схем и механизмов безопасности — занятие увлекательное и в определенной степени необходимое, но едва ли имеет смысл тратить деньги и время на такую проработку, если без внимания остались простые регуляторы. Например, как бы тщательно ни была продумана система, построенная на основе существующих средств безопасности, один пользователь с плохо выбранным паролем способен поставить под удар всю организацию.

3.4. Используйте несколько стратегий защиты активов

Другой метод защиты активов состоит в использовании нескольких стратегий.

При подобном подходе, если одна линия обороны оказывается прорванной, в дело

вступает другая стратегия, то есть активы не остаются беззащитными. Комбинация нескольких несложных стратегий зачастую позволяет построить более надежную защиту, чем один, даже очень сложный, метод. Так, дополнением к традиционному механизму входа в систему могут служить модемы с обратным дозвоном, и число подобных примеров многоуровневой защиты активов можно умножать. Правда, с комбинированием стратегий легко переборщить, поэтому следует постоянно помнить, что же собственно защищается.

3.5. Физическая безопасность

Давно известно, что если не обеспечена физическая защита, говорить о других аспектах информационной безопасности не имеет смысла. Имея физический доступ к машине, злоумышленник может остановить ее, перевызвать в привилегированном режиме, заменить диск или изменить его содержимое, внедрить "Троянского коня" (см. п. 2.13.9.2) или предпринять любое число других нежелательных акций, предотвратить которые крайне трудно.

Критически важные коммуникационные каналы, серверы и другие ключевые элементы должны быть сосредоточены в физически защищенных областях. Некоторые механизмы безопасности (например, сервер аутентификации Kerberos) выполняют свои функции только при условии физической защищенности.

Если Вы не можете физически обезопасить машины, не следует слепо доверять им. Целесообразно ограничить доступ с менее защищенных машин в более защищенные. Особенно рискованно предоставлять незащищенным хостам право доверительного доступа (как в ОС UNIX посредством удаленных команд типа rsh).

Необходимо строго контролировать доступ к физически защищенным машинам или претендующим на звание таковых. Помните, что у технического и обслуживающего персонала, как правило, есть ключи от комнат.

3.6. Процедуры выявления неавторизованной деятельности

Для обнаружения большинства видов неавторизованного использования компьютерных систем существуют несложные процедуры, использующие стандартные средства операционных систем или опирающиеся на инструментарий, свободно доступный из различных источников.

3.6.1. Отслеживание использования систем

Системный мониторинг может выполняться как администратором, так и специально написанными программами. Мониторинг включает в себя просмотр различных частей системы в поисках чего-нибудь необычного. Некоторые простые способы решения данной задачи будут рассмотрены ниже.

Отслеживание использования систем очень важно выполнять на постоянной основе. Бессмысленно выделять для мониторинга один день в месяце, поскольку нарушения режима безопасности зачастую длятся всего несколько часов. Только поддерживая постоянную бдительность, можно рассчитывать на своевременную реакцию на нарушения.

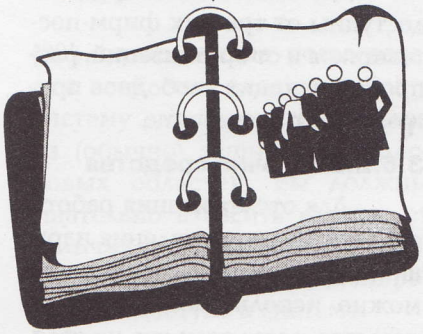
3.6.2. Инструменты для отслеживания использования систем

В данном пункте описываются инструменты и методы, позволяющие выявлять неавторизованное использование систем.

3.6.2.1. Ведение регистрационных журналов

Большинство операционных систем сохраняют в регистрационных файлах массу информации. Регулярный анализ этих файлов обычно является первой линией обороны при определении неавторизованного использования систем.

- Сравните текущий список активных пользователей с предыдущими записями о входах в систему. Большинство пользователей каждый день входят в систему и выходят из нее приблизительно в одно и то же время. Вход в "ненормальное" время может свидетельствовать об использовании системного счета злоумышленником.
- Во многих системах накапливаются учетные записи с целью последующего выставления счетов. Эти записи также можно использовать для определения типичного профиля использования системы. Необычные записи могут быть следствием неавторизованной активности.



- Обычно в системах существуют средства накопления регистрационной информации (например, "syslog" в ОС UNIX). Проверьте эту информацию на предмет необычных сообщений об ошибках, генерируемых программным обеспечением. Например, большое число неудачных попыток входа в течение короткого промежутка времени может свидетельствовать о попытках подобрать пароль.
- С помощью команд операционной системы, выводящих список выполняемых в данный момент процессов, можно выявить пользователей, запустивших программы, к которым они не имеют права обращаться, равно как и неавторизованные программы, запущенные нарушителем.

3.6.2.2. Программы отслеживания

Другие средства мониторинга можно сконструировать, комбинируя различные, на первый взгляд не связанные между собой, стандартные механизмы операционной системы. Например, контрольный список прав доступа к файлам и их владельцев в ОС UNIX нетрудно получить с помощью команд "find" и "ls" и сохранить как эталон. Затем периодически можно порождать новые списки и сравнивать их с эталоном (в ОС UNIX для этого имеется команда "diff"). Несовпадения, возможно, свидетельствуют о несанкционированных изменениях.

Дополнительные средства доступны от третьих фирм-поставщиков и от организаций, распространяющих свободное программное обеспечение.

3.6.2.3. Прочие средства

Для отслеживания работы систем с целью выявления нарушений режима безопасности можно использовать и другие средства, даже если это не является их основным назначением. Например, сетевые мониторы способны обнаружить и зарегистрировать соединения от неизвестных организаций.

3.6.3. Меняйте расписание мониторинга

Задача системного мониторинга — не такая страшная, как могло бы показаться. Системные администраторы могут выполнять многие команды, используемые для мониторинга, периодически в течение дня, заполняя ими паузы (например, во время телефонного разговора). Это лучше, чем действовать строго по расписанию, При частом выполнении команд Вы быстрее привыкнете к "нормальным" результатам и будете легче обнаруживать аномалии. Кроме того, варьируя время мониторинга, Вы сделаете Ваши действия менее предсказуемыми для злоумышленников. Например, если злоумышленник знает, что каждый день в 17:00 проверяется, все ли вышли из системы, он просто переждет момент проверки и войдет позже. Но он не может предсказать, когда системный администратор выполнит команду вывода списка активных пользователей. Тем самым риск быть обнаруженным для злоумышленника существенно возрастает.

Несмотря на достоинства, которыми обладает постоянный мониторинг, некоторые злоумышленники могут знать о стандартных регистрационных механизмах атакуемых систем. В результате возможно активное противодействие и выведение этих механизмов из строя. Таким образом, обычное отслеживание полезно для обнаружения нарушителей, но оно не гарантирует безопасности Вашей системы, как не гарантирует оно и безошибочного выявления неавторизованных действий.

3.7. Что делать при подозрениях на неавторизованную деятельность

В разделах 2.4 и 2.5 обсуждался характер действий, предпринимаемых организацией при подозрениях на нарушение режима информационной безопасности. Политика безопасности должна описывать общий подход к подобным проблемам.

В дополнение к политике, необходимо выписать процедуры реагирования на вторжения. Кто имеет право решать, что именно делать? Следует ли обращаться в правоохранительные органы? Должна ли Ваша организация сотрудничать с другими предприятиями в попытках выследить нарушителя? Ответы на все эти вопросы, выбранные в соответствии с рекомендациями из раздела 2.4, должны стать частью процедур безопасности.

Независимо от того, предпочтете ли Вы пресекать действия нарушителя или следить за ним, Вам необходимо держать наготове соответствующие инструменты, предварительно научившись ими пользоваться. Не ждите вторжения, чтобы овладеть методами отслеживания действий злоумышленников; Вам будет не до того.

3.8. Оглашая политику безопасности

Чтобы политика безопасности действительно работала, ее необходимо довести до сведения пользователей и системных администраторов. В данном разделе объясняется, что и как следует говорить этим людям.

3.8.1. Обучая пользователей

Пользователи должны знать, как правильно использовать компьютерные системы и как защитить себя от неавторизованных лиц.

3.8.1.1. Правильное использование системных счетов и/или рабочих станций

Всем пользователям необходимо разъяснить, что подразумевается под "правильным" использованием системных счетов и рабочих станций (см. п. 2.3.2). Проще всего это сделать, когда пользователь получает новый счет и, одновременно, брошюру с текстом политики безопасности. Политика использования обычно должна определять, разрешается ли применять счет или рабочую станцию для личных надобностей (ведение домашней бухгалтерии, подготовка писем), для извлечения доходов, для игр и т.д. В политике могут также содержаться положения, касающиеся лицензионных вопросов. Например, многие университеты имеют учебные лицензии, явным образом запрещающие коммерческое использование систем. Более полный список тем, составляющих данный аспект политики безопасности, приведен в разделе 2.3.

3.8.1.2. Процедуры администрирования счета и/или рабочей станции

Каждому пользователю необходимо объяснить, как правильно администрировать счет и/или рабочую станцию. В частности, пользователь должен усвоить, как защищать файлы, как выходить из системы или блокировать терминал или рабочую станцию и т.п. По большей части подобная информация содержится в документации для новичков, поставляемой вместе с операционной системой, хотя во многих организациях предпочитают делать свои дополнения, учитывающие местную специфику.

Если компьютеры Вашей организации открыты для модемного доступа по коммутируемым линиям, необходимо проинформировать пользователей об опасностях, присущих подобным конфигурациям. Например, прежде чем получить право на модемный доступ, пользователи должны усвоить, что следует сначала выходить из системы и только потом вешать трубку.

Аналогично, наличие доступа к системе через локальные или глобальные сети несет с собой свой набор проблем безопасности, которые нужно довести до сведения пользователей. Файлы, придающие статус доверенных удаленным хостам или пользователям, должны быть изучены досконально.

3.8.1.3. Выявление нелегального использования счета

Пользователям необходимо объяснить, как выявлять случаи нелегального использования их счетов. Если при входе в систему выдается время предыдущего входа, пользователи должны его контролировать на предмет согласованности со своими прошлыми действиями.

Командные интерпретаторы некоторых операционных систем (например, C-shell в ОС UNIX) поддерживают историю выполнения команд. Целесообразно время от времени заглядывать в историю, чтобы проверять, не пользовались ли данным счетом другие лица для выполнения своих команд.

3.8.1.4. Процедуры доклада о проблемах

Должны быть разработаны процедуры, позволяющие пользователям докладывать о замеченных проблемах, связанных с неправильным использованием счета или с другими аспектами безопасности. Пользователям следует сообщить имя и телефон администратора безопасности или соответствующий адрес электронной почты (например, "security").

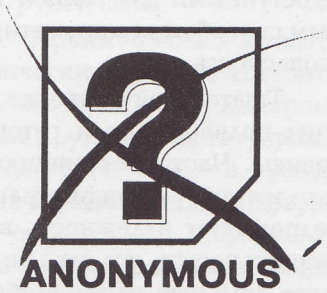
3.8.2. Обучая администраторов хостов

Во многих организациях компьютерные системы администрируются самыми разными людьми. Эти люди должны знать, как защищать свою систему от атак и неавторизованного использования и как сообщать о случаях успешного проникновения в назидание коллегам.

3.8.2.1. Процедуры администрирования счетов

Администрирование счетов требует осторожности. При начальной установке системы с дистрибутива следует проверить элементы файла паролей, соответствующие "стандартным" счетам, заведенным поставщиком. Многие поставщики заводят счета для административного и обслуживающего персонала вообще без паролей или с общеизвестными паролями. Следует или дать новые пароли, или аннулировать ненужные счета.

Иметь счета без паролей очень опасно, поскольку они открывают свободный доступ в систему. Даже счета, при входе по которым запускается не командный интерпретатор, а другая программа (например, программа вывода списка активных пользователей) могут быть скомпрометированы, если установки выполнены некорректно. Опасны и средства "анонимной" передачи файлов (FTP)



[20], позволяющие пользователям всей сети входить в Вашу систему для перекачки файлов из (обычно) защищенных дисковых областей. Вы должны тщательно взвесить выгоды от наличия счета без пароля в сравнении с риском несанкционированного доступа к системе.

Если операционная система поддерживает "теневые" файлы паролей (хранение паролей в отдельных файлах, доступных только привилегированным пользователям), ими нужно обязательно воспользоваться. В число таких систем входят UNIX System V, SunOS 4.0 или старше и некоторые другие. Поскольку зашифрованные пароли оказываются недоступны обычным пользователям, нападающий не сможет скопировать их на свою машину, чтобы на досуге заняться их раскрытием.

Отслеживайте использование привилегированных счетов ("root" в ОС UNIX или "MAINT" в VMS). Как только привилегированный пользователь увольняется или перестает нуждаться в привилегиях, следует изменить пароли всех привилегированных счетов.

3.8.2.2. Процедуры конфигурационного управления

При установке с дистрибутива операционной системы или дополнительного программного продукта необходимо тщательно проверить результирующую конфигурацию. Многие процедуры установки исходят из предположения надежности всех пользователей в организации, оставляя файлы общедоступными для записи или иным способом компрометируя безопасность.

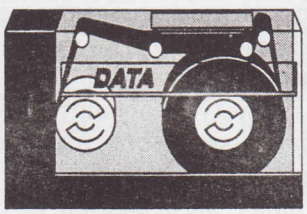
Тщательной проверке должны подвергаться и сетевые сервисы. Часто поставщики в стандартной конфигурации предполагают надежность всех внешних хостов, что едва ли разумно, если речь идет о глобальной сети, такой как Интернет.

Многие злоумышленники собирают информацию о слабостях конкретных версий систем. Чем старее версия, тем более вероятно наличие в ее защите известных ошибок, исправленных поставщиком в более поздних выпусках. В этой связи необходимо сопоставить риск от сохранения старой версии (с "дырами" в безопасности) и стоимость перехода на новое программное обеспечение (включая возможные проблемы с продуктами третьих фирм). Из тех же соображений оценивается и целесообразность постановки "заплат", предоставляемых поставщиком, но с учетом того обстоятельства, что заплаты к системе безопасности, как правило, закрывают действительно серьезные дыры.

Другие исправления, полученные по электронной рассылке или аналогичным образом, обычно следует вносить, но только после тщательной проверки. Никогда не вносите исправления, если не уверены, что понимаете все последствия. Всегда есть опасность, что "исправление" предлагает злоумышленник, дабы открыть себе доступ в Вашу систему.

3.8.2.3. Процедуры сохранения и восстановления

Невозможно переоценить важность хорошей стратегии резервного копирования. Наличие копии файловой системы не только выручит Вас в случае поломки аппаратуры или нечаянного удаления данных, но и защитит от последствий несанкционированных изменений, внесенных злоумышленником. Без копии, действуя только по методу "максимального правдоподобия", трудно вернуть к первоначальному состоянию все то, что было злонамеренно модифицировано.



Резервные копии, особенно ежедневные, могут быть полезны и для прослеживания действий злоумышленника. Анализируя старые копии, нетрудно выяснить, когда система была скомпрометирована в первый раз. Нарушитель мог оставить следы в виде файлов, впоследствии удаленных, но оставшихся на копии. Резервные копии — это и материал для правоохранительных органов, расследующих компьютерные преступления.

Хорошая стратегия состоит в том, чтобы делать полную копию не реже одного раза в месяц. Частичные (или "инкрементальные") должны делаться не реже двух раз в неделю, а в идеале — каждый день. Предпочтительно использовать команды, специально предназначенные для сохранения файловых систем ("dump" в случае ОС UNIX или "BACKUP" на VMS), а не просто команды копирования файлов, поскольку первые обеспечивают возможность восстановления целостного состояния.

3.8.2.4. Процедуры доклада о проблемах

Как и пользователи, администраторы должны располагать конкретными процедурами доклада о проблемах, связанных с информационной безопасностью. Для больших конфигураций обычно заводят список электронной рассылки, в котором перечисляются все системные администраторы организации. Можно также организовать группу быстрого реагирования по типу CERT или горячую линию, обслуживаемую группой поддержки.

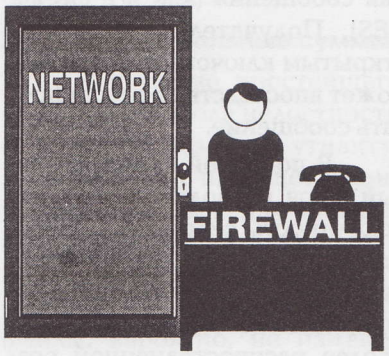
3.9. Ресурсы для предупреждения нарушений безопасности

В этом разделе обсуждаются программные, аппаратные и процедурные ресурсы, которые могут быть использованы для поддержки Вашей политики безопасности.

3.9.1. Сетевые соединения и межсетевые экраны

Противопожарные перегородки (firewalls) устанавлива-

ют в зданиях, чтобы воспрепятствовать проникновению пламени в защищаемые области. (В русском языке получил распространение также термин "брандмауэр", обозначающий устройство аналогичного назначения в автомобиле. Оно защищает салон в случае возгорания двигателя. Применительно к компьютерным вопросам мы будем использовать термин "межсетевой экран".) Аналогично, секретариат или приемная являются точками контроля за доступом посетителей в другие части офиса. По-



добную технологию можно распространить и на информационную систему предприятия, особенно если речь идет о сетевых соединениях.

Некоторые сети соединяются только с другими сетями той же организации и не имеют выхода во внешний мир. Подобные организации менее уязвимы для угроз извне, хотя злоумышленник все же может воспользоваться коммуникационными каналами (например, коммутируемыми телефонными линиями). С другой стороны, многие организации связаны с другими предприятиями через глобальные сети, такие как Интернет. Над такими организациями нависают все опасности, типичные для сетевых сред.

Перед подключением к внешним сетям следует взвесить все "за" и "против". Разумно сделать доступными из внешнего мира только хосты, не хранящие критичной информации, изолируя жизненно важные машины (например, с данными о финансовых или материальных ценностях). Если необходимо включиться в глобальную сеть, рассмотрите возможность ограничения доступа к Вашей локальной сети через один хост. Иными словами, все информационные потоки из Вашей локальной сети и в нее должны проходить через один хост, играющий роль противопожарной перегородки между Вашей организацией и внешним миром. Эту экранирующую систему необходимо строго контролировать, защищать паролями, а функциональные возможности, доступные внешним пользователям, следует ограничить. С помощью такого подхода Ваша организация сможет ослабить некоторые внутренние регуляторы безопасности в локальной сети, сохраняя прочно защищенный передний край.

Заметьте, что даже при наличии межсетевого экрана его компрометация может привести к компрометации всей прикрываемой локальной сети. Ведутся работы по созданию экранирующих систем, которые, даже будучи скомпрометированы, все же защищают локальную сеть [6].

3.9.2. Конфиденциальность

Конфиденциальность, то есть обеспечение скрытности или секретности, — одна из главных практических целей информационной безопасности. Большинство современных операционных систем предоставляют различные механизмы, которые дают пользователям возможность контролировать распространение информации. В зависимости от своих нужд, организация может защищать все, может, напротив, все считать общедоступным или занимать место где-то в середине спектра, что большинство организация и делает (во всяком случае, до первого нарушения режима безопасности).

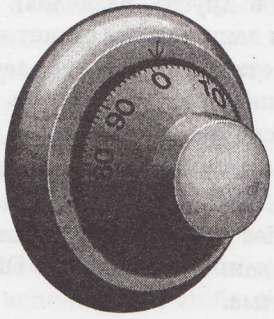
Как правило, с информацией могут несанкционированно ознакомиться в трех местах — там, где она хранится (на компьютерных системах), там, где она передается (в сети) и там, где хранятся резервные копии (на лентах).

В первом случае для защиты используются права доступа к файлам, списки управления доступом и/или аналогичные механизмы. В последнем случае можно применить физическое ограничение доступа к лентам (например, заперев их в сейф). И во всех случаях помощь способны оказать криптографические средства.

3.9.2.1. Шифрование (аппаратное и программное)

Шифрование — это процесс преобразования информации из читабельной формы в нечитабельную. Коммерчески доступны несколько криптографических пакетов, где шифрование реализовано аппаратно или программно. Аппаратное шифрование значительно быстрее программного; однако это достоинство может обернуться и недостатком, так как криптографические устройства могут стать объектом атаки злоумышленника, пожелавшего расшифровать Вашу информацию методом грубой силы.

Преимущество криптографических методов состоит в том, что даже после компрометации других средств управления доступом (паролей, прав доступа к файлам и т.п.) информация остается для злоумышленника бесполезной. Естественно, ключи шифрования и аналогич-



ные атрибуты должны защищаться не менее тщательно, чем файлы паролей.

Передаваемую по сети информацию могут перехватить. Для защиты от этой угрозы существует несколько методов, начиная от простого шифрования файлов перед передачей (шифрование из конца в конец) и кончая использованием специального сетевого оборудования, шифрующего всю передаваемую информацию без вмешательства пользователя (секретные каналы). Интернет в целом не использует секретные каналы, поэтому, если возникает необходимость, приходится использовать шифрование из конца в конец.

3.9.2.1.1. Стандарт шифрования данных (Data Encryption Standard, DES)

Пожалуй, на сегодняшний день DES является наиболее употребительным механизмом шифрования. Существует ряд аппаратных и программных реализаций этого механизма, а некоторые компьютеры поставляются вместе с программной версией. DES преобразует обычный текст в шифрованный посредством специального алгоритма и "затравки", называемой ключом. До тех пор, пока пользователь хранит (или помнит) ключ, он может вернуть текст из шифрованного состояния в обычное.

Одна из потенциальных опасностей любой системы шифрования состоит в необходимости помнить ключ, с помощью которого текст был зашифрован (это напоминает проблему с паролями, обсуждаемую в других разделах). Если ключ записать, он станет менее секретным. Если его забыть, расшифровка становится практически невозможной.

Большинство вариантов ОС UNIX предоставляют команду "des", позволяющую шифровать данные с помощью DES-алгоритма.

3.9.2.1.2. Crypt

Как и команда "des", команда "crypt" ОС UNIX позволяет шифровать информацию. К сожалению, алгоритм, использованный в реализации "crypt", весьма ненадежен (он заимствован из шифровального устройства "Enigma" времен второй мировой войны), так что файлы, зашифрованные данной командой, нетрудно расшифровать за несколько часов. Пользоваться командой "crypt" не рекомендуется, за исключением особо тривиальных случаев.

3.9.2.2. Конфиденциальная почта (Privacy Enhanced Mail, PEM)

Обычно электронная почта передается по сети в открытом виде (то есть прочитать ее может каждый). Такое решение, конечно, нельзя назвать идеальным. Конфиденциальная почта предоставляет средства для автоматического шифрования электронных сообщений, так что лицо, осуществляющее прослушивание в узле распределения почты, не сможет (легко) эти сообщения прочитать. В настоящее время разрабатывается и распространяется по Интернет несколько пакетов конфиденциальной почты.

Группа по конфиденциальности сообщества Интернет разрабатывает протокол, предназначенный для использования в реализациях конфиденциальной почты. См. RFC 1113, 1114, 1115 [7, 8, 9].

3.9.3. Аутентификация источника данных

Обычно мы принимаем на веру, что в заголовке электронного сообщения отправитель указан правильно. Заголовок, однако, нетрудно подделать. Аутентификация источника данных позволяет удостоверить подлинность отправителя сообщения или другого объекта, подобно тому, как нотариус заверяет подпись на официальном документе. Цель достигается с помощью систем шифрования с открытыми ключами.

Шифрование с открытыми ключами отличается от систем с секретными ключами несколькими моментами. Во-первых, в системе с открытыми ключами применяются два ключа — открытый, который каждый может использовать (иногда такой ключ называют публичным), и секретный, известный только отправителю сообщения. Отправитель использует секретный ключ для шифрования сообщения (как и в случае DES). Получатель, располагая открытым ключом отправителя, может впоследствии расшифровать сообщение.

В подобной схеме открытый ключ позволяет проверить подлинность секретного ключа отправителя. Тем самым более строго доказывается подлинность самого отправителя. Наиболее распространенной реализацией схемы шифрования с открытыми ключами является система RSA [26]. Она использована и в стандарте Интернет на конфиденциальную почту (PEM).

3.9.4. Целостность информации

Говорят, что информация находится в целостном состоянии, если она полна, корректна и не изменилась с момента последней проверки "цельности". Для разных организаций важность целостности данных различна. Например, для военных и правительственных организаций сохранение режима секретности гораздо важнее истинности информации. С другой стороны, для банка важна прежде всего полнота и точность сведений о счетах своих клиентов.

На целостность системной информации влияют многочисленные программно-технические и процедурные механизмы. Традиционные средства управления доступом обеспечива-

ют контроль над тем, кто имеет доступ к системной информации. Однако, не всегда эти механизмы сами по себе достаточны для обеспечения требуемого уровня целостности. Ниже кратко обсуждаются некоторые дополнительные средства.

Заметим, что, помимо обсуждаемых, имеются и другие механизмы обеспечения целостности, такие как совместный контроль со стороны двух лиц и процедуры проверки целостности. К сожалению, их рассмотрение выходит за рамки настоящего документа.

3.9.4.1. Контрольные суммы

В качестве простейшего средства контроля целостности можно использовать утилиту, которая подсчитывает контрольные суммы для системных файлов и сравнивает их с предыдущими известными значениями. В случае совпадения файлы, вероятно, не изменились; при несовпадении можно утверждать, что кто-то изменил их некоторым неизвестным способом.

Оборотной стороной простоты и легкости реализации является ненадежность механизма контрольного суммирования. Целенаправленный злоумышленник без труда добавит в файл несколько символов и получит требуемое значение суммы.

Особый тип контрольных сумм, называемый циклическим контролем (Cyclic Redundancy Check, CRC) обладает гораздо большей надежностью. Его реализация лишь немногим сложнее, зато обеспечивается более высокая степень контроля. Тем не менее, и он может не устоять перед злоумышленником.

Контрольные суммы можно использовать для обнаружения фактов изменения информации, однако они не обеспечивают активной защиты от внесения изменений. По этой причине следует применять другие механизмы, такие как управление доступом и криптография.

3.9.4.2. Криптографические контрольные суммы

Криптографические контрольные суммы (называемые также имитовставками) вычисляются следующим образом. Файл делится на порции, для каждой из них подсчитывается контрольная сумма (CRC), а затем эти частичные суммы складываются. При подходящей реализации данный метод гарантирует практически стопроцентное обнаружение изменений файлов, несмотря на возможное противодействие злоумышленника. Недостаток метода состоит в том, что он требует значительных вычислительных ресурсов, так что его разумно применять лишь тогда, когда требуется максимально возможный контроль целостности.

Другой сходный механизм, называемый односторонней хэш-функцией (или кодом обнаружения манипуляций, Manipulation Detection Code, MDC), может быть использован также для уникальной идентификации файлов. Идея состоит в том, что никакие два разных исходных файла не дадут одинаковых результатов, так что при модификации файла хэш-функция изменит значение. Односторонние хэш-функции допускают эффективную реализацию на самых разных системах, что превращает стопроцентное обнаружение изменений файлов в реальность. (Одним из примеров эффективной односторонней хэш-функции является Snefru, доступная по USENET и Интернет [10].)

3.9.5. Ограничение сетевого доступа

Протоколы, доминирующие в Интернет, — IP (RFC 791) [11], TCP (RFC 793) [12] и UDP (RFC 768) [13] — предусматривают наличие управляющей информации, которой можно воспользоваться для ограничения доступа к определенным хостам или сетям организации.

Заголовок IP-пакета содержит сетевые адреса как отправителя, так и получателя. Далее, протоколы TCP и UDP поддерживают понятие "порта", идентифицирующего оконечную точку коммуникационного маршрута (обычно это сетевой сервер). В некоторых случаях может быть желательным запретить доступ к конкретным TCP- или UDP-портам, а, быть может, даже к определенным хостам или сетям.

3.9.5.1. Шлюзовые маршрутные таблицы

Один из простейших способов предотвращения нежелательных сетевых соединений состоит в удалении определенных сетей из шлюзовых маршрутных таблиц. В результате хост лишается возможности послать пакеты в эти сети. (В большинстве протоколов предусмотрен двусторонний обмен пакетами даже при однонаправленном информационном потоке, поэтому нарушения маршрута с одной стороны обычно бывает достаточно.)

Подобный подход обычно применяется в экранирующих системах, чтобы не открывать локальные маршруты для внешнего мира. Правда, при этом зачастую запрещается слишком много (например, для предотвращения доступа к одному хосту закрывается доступ ко всем системам сети).

3.9.5.2. Фильтрация пакетов маршрутизатором

Многие коммерчески доступные шлюзовые системы (которые более правильно называть маршрутизаторами) предоставляют возможность фильтрации пакетов, основываясь не только на адресах отправителя или получателя, но и на их комбинациях. Этот подход может быть использован, чтобы запре-

тить доступ к определенному хосту, сети или подсети из другого хоста, сети или подсети.

Шлюзовые системы некоторых поставщиков (например, Cisco Systems) поддерживают еще более сложные схемы, допуская более детальный контроль над адресами отправителя и получателя. Посредством масок адресов можно запретить доступ ко всем хостам определенной сети, кроме одного. Маршрутизаторы Cisco Systems реализуют также фильтрацию пакетов на основе типа IP-протокола и номеров TCP- или UDP-портов [14].

Для обхода механизма фильтрации злоумышленник может воспользоваться "маршрутизацией отправителем". Возможно отфильтровать и такие пакеты, но тогда под угрозой окажутся некоторые законные действия (например, диагностические).

3.9.6. Системы аутентификации

Аутентификация — это процесс проверки подлинности "личности", проводимый в нтересах инстанции, распределяющей полномочия. Системы аутентификации могут включать в себя аппаратные, программные и процедурные механизмы, которые дают возможность пользователю получить доступ к вычислительным ресурсам. В простейшем случае частью механизма аутентификации является системный администратор, заводящий новые пользовательские счета. На другом конце спектра находятся высокотехнологичные системы распознавания отпечатков пальцев и сканирования роговицы потенциальных пользователей. Без доказательного установления личности пользователя до начала сеанса работы, компьютеры Вашей организации будут уязвимы по существу для любых атак.

Обычно пользователь доказывает свою подлинность системе, вводя пароль в ответ на приглашение. Запросно-ответные системы улучшают парольную схему, предлагая ввести элемент данных, известный и компьютерной системе, и пользователю (например, девичью фамилию матери и т.п.).

3.9.6.1. Kerberos

Система Kerberos, названная по имени мифологического пса, охранявшего врата ада, является набором программ, используемых в больших сетях для проверки подлинности пользователей. Разработанная в Массачусетском технологическом институте, она опирается на криптографию и распределенные базы данных и дает возможность пользователям распределенных конфигураций начинать сеанс и работать с любого компьютера. Очевидно, это полезно в учебном или аналогичном ему окружении, когда большое число потенциальных пользователей могут инициировать подключение с любой из множества рабочих станций. Некоторые поставщики встраивают Kerberos в свои системы.

Заметим, что несмотря на сделанные улучшения в механизме аутентификации, в протоколе Kerberos остались уязвимые места [15].

3.9.6.2. Интеллектуальные карты

В некоторых системах для облегчения аутентификации применяются "интеллектуальные карты" (небольшие устройства размером с калькулятор). Здесь подлинность пользователя подтверждается обладанием определенным объектом. Одна из разновидностей такой системы включает в себя новую парольную процедуру, когда пользователь вводит значение, полученное от "интеллектуальной карты". Обычно хост передает пользователю элемент данных, который следует набрать на клавиатуре карты. Интеллектуальная карта высвечивает на дисплее ответ, который, в свою очередь, нужно ввести в компьютер. Только после этого начинается сеанс работы. Другая разновидность использует интеллектуальные карты, высвечивающие меняющиеся со временем числа. Пользователь вводит текущее число в компьютер, где аутентификационное программное обеспечение, синхронизированное с картой, проверяет корректность введенного значения.

Интеллектуальные карты обеспечивают более надежную аутентификацию по сравнению с традиционными паролями. С другой стороны, использование карт сопряжено с некоторыми неудобствами, да и начальные затраты довольно велики.

4. Типы процедур безопасности

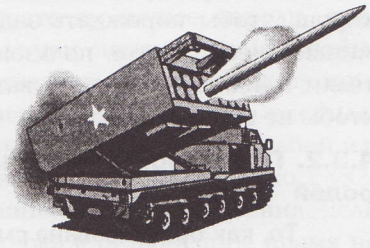
4.1. Проверка системной безопасности

Частью нормальной деловой жизни многих бизнесменов являются ежегодные финансовые проверки. Проверки безопасности — важная часть функционирования любой компьютерной среды. Элементом таких проверок должна стать ревизия политики безопасности и защитных механизмов, используемых для проведенияполитики в жизнь.

4.1.1. Проводите плановые учения

Конечно, не каждый день или каждую неделю, но периодически нужно проводить плановые учения, чтобы проверить, адекватны ли выбранные процедуры безопасности предполага-

емым угрозам. Если главной угрозой Вы считаете стихийное бедствие, на учении могут проверяться механизмы резервного копирования и восстановления. С другой стороны, если Вы опасаетесь прежде всего вторжения в систему сторонних злоумышленников, можно устроить учебную атаку, проверив тем самым эффективность политики безопасности.



Учения — хороший способ выяснения результативности политики и процедур безопасности. С другой стороны, они отнимают много времени и нарушают нормальную работу. Важно сопоставлять выгоды от учений и неизбежно связанные с ними потери времени.

4.1.2. Проверяйте процедуры

Если решено не устраивать плановых учений, проверяющих сразу всю систему безопасности, следует как можно чаще проверять отдельные процедуры. Проверьте процедуру резервного копирования, чтобы убедиться, что Вы можете восстановить данные с лент. Проверьте регистрационные журналы, чтобы удостовериться в их полноте и т.п.

При проведении проверок необходимо с максимальной тщательностью подбирать тесты политики безопасности. Важно четко определить, что тестируется, как проводится тестирование и какие результаты ожидаются. Все это нужно документировать и включить в основной текст политики безопасности или издать в качестве дополнения.

Важно протестировать все аспекты политики безопасности, процедурные и программно-технические, с упором на автоматизированные механизмы проведения политики в жизнь. Должна быть уверенность в полноте тестирования каждого средства защиты. Например, если проверяется процесс входа пользователя в систему, следует явно оговорить, что будут пробоваться правильные и неправильные входные имена и пароли.

Помните, что существует предел разумности тестирования. Цель проверок состоит в получении уверенности, что политики безопасности корректно проводится в жизнь, а не в "доказательстве абсолютной правильности" системы или политики. Важно убедиться, что разумные и надежные средства защиты, предписанные политикой, обеспечивают должный уровень безопасности.

4.2. Процедуры управления счетами

Процедуры управления счетами важны для предотвращения несанкционированного доступа к Вашей системе. В этой связи в политике безопасности необходимо дать ответы на следующие вопросы:

- Кто может иметь счет на данной системе?
- Как долго можно иметь счет без обновления запроса?
- Как из системы удаляются старые счета?

Помимо определения круга возможных пользователей, необходимо решить, для чего каждый из них имеет право использовать систему (например, допускается ли применение в личных целях). Если имеется подключение к внешней сети, то ее или Ваше руководство могут установить правила пользования этой сетью. Следовательно, для любой политики безопасности важно определить подходящие процедуры управления счетами как для администраторов, так и для пользователей. Обычно системный администратор отвечает за заведение и ликвидацию счетов и осуществляет общий контроль за использованием системы. До некоторой степени, управление счетом — обязанность каждого пользователя, в том смысле, что он должен следить за всеми системными сообщениями и событиями, которые могут свидетельствовать о нарушении политики безопасности. Например, выдаваемое при входе в систему сообщение с датой и временем предыдущего входа необходимо переправить "куда следует", если оно не согласуется с прошлыми действиями пользователя.

4.3. Процедуры управления паролями

Политика управления паролями важна для поддержания их секретности. Соответствующие процедуры могут варьироваться от эпизодических просьб или приказаний пользователю сменить пароль, до активных попыток этот пароль подобрать с последующим информированием владельца о легкости данного мероприятия. Другая часть политики управления описывает, кто может распространять пароли — имеет ли право пользователь сообщать свой пароль другим?

В разделе 2.3 обсуждались некоторые политические решения, которые необходимо принять для правильного управления паролями. Независимо от политики, процедуры управления должны быть тщательно продуманы и подробно регламентированы, чтобы избежать раскрытия паролей. Критичным является выбор начальных паролей. Бывают случаи, когда пользователи вообще не работают в системе и, следовательно, не активируют счета. Значит, начальный пароль не должен быть очевидным. Никогда не присваивайте счетам пароли "по умолчанию", каждый раз придумывайте новый пароль. Если существует печатный спи-

сок паролей, его необходимо хранить подальше от посторонних глаз в надежном месте. Впрочем, лучше вообще обойтись без подобного списка.

4.3.1. Выбор пароля

Пожалуй, пароли — наиболее уязвимая часть любой компьютерной системы. Как бы ни была защищена система от атак по сети или по коммутируемым линиям, от "Троянских коней" и аналогичных опасностей, она может быть полностью скомпрометирована злоумышленником, если тот получит к ней доступ из-за плохо выбранного пароля. Важно сформировать хороший свод правил выбора паролей, и довести его до каждого пользователя. По возможности, следует модифицировать программное обеспечение, устанавливающее пароли, чтобы оно в максимальной степени поддерживало эти правила.

Ниже приведен набор простых рекомендаций по выбору паролей.

- НЕ используйте в качестве пароля производные от входного имени (само имя, обращенное, записанное прописными буквами, удвоенное имя и т.п.).
- НЕ используйте в качестве пароля свое имя, отчество или фамилию.
- НЕ используйте имя супруги (супруга) или детей.
- НЕ используйте другую ассоциированную с Вами информацию, которую легко узнать (номера документов и телефонов, марку автомобиля, домашний адрес и т.п.).
- НЕ используйте чисто цифровой пароль или пароль из повторяющихся букв.
- НЕ используйте слов, содержащихся в словаре английского или иного языка, в других списках слов.
- НЕ используйте пароль менее чем из шести символов.
- ИСПОЛЬЗУЙТЕ пароли со сменой регистра букв.
- ИСПОЛЬЗУЙТЕ пароли с небуквенными символами (цифрами или знаками пунктуации).
- ИСПОЛЬЗУЙТЕ запоминающиеся пароли, чтобы не пришлось записывать их на бумаге.
- ИСПОЛЬЗУЙТЕ пароли, которые Вы можете ввести быстро, не глядя на клавиатуру.

Методы выбора пароля в соответствии с приведенными рекомендациями могут состоять в следующем.

- Возьмите одну-две строки из песни или стихотворения и составьте пароль из первых букв последовательных слов.
- Составьте последовательность из чередующихся согласных и гласных (одной или двух подряд) букв длиной семь-восемь символов. Получится бессмысленное, но легко произносимое и, следовательно, запоминающееся слово.
- Выберите два коротких слова и соедините их, вставив в середину знак пунктуации.

Пользователей нужно убедить в необходимости регулярно менять пароли, обычно раз в три-шесть месяцев. Это позволяет поддерживать уверенность в том, что даже если злоумышленник подберет один из паролей, он в конце концов потеряет доступ к системе, равно как рано или поздно потеряет актуальность нелегально полученный список паролей. Многие системы дают администратору возможность заставлять пользователей менять пароли по истечении срока годности; если Вам доступно соответствующее программное обеспечение, его нужно задействовать [5].

Некоторые системы программным образом вынуждают пользователей регулярно менять пароли. Компонентом многих из подобных систем является генератор паролей. Он предлагает пользователю на выбор несколько вариантов; самостоятельно придумывать пароли не разрешается. У таких систем есть как достоинства, так и недостатки. С одной стороны, генерация защищает от выбора слабых паролей. С другой стороны, если генератор не настолько хорош, чтобы порождать запоминающиеся пароли, пользователям придется их записывать, чтобы не забыть.

4.3.2. Процедуры смены паролей

То, как организована смена паролей, существенно для их безопасности. В идеале, у пользователей должна быть возможность менять пароли в оперативном режиме. (Имейте в виду, что программы смены паролей — излюбленная мишень злоумышленников. Более подробную информацию можно найти в разделе 4.4, посвященном конфигурационному управлению.)

Бывают, однако, исключительные случаи, когда действовать нужно осторожно. Пользователь может забыть пароль и лишиться тем самым возможности входа в систему. Стандартная процедура состоит в присваивании пользователю нового пароля. При этом важно убедиться, что запрашивает смену и получает новый пароль реальный человек. Одна из стандартных уловок злоумышленников — позвонить или послать сообщение системному администратору и запросить новый пароль. Перед выдачей нового пароля нужно применить какую-либо внешнюю форму проверки подлинности пользователя. В некоторых организациях пользователи должны лично явиться к администратору, имея при себе удостоверение.

Иногда нужно изменить много паролей. Если система скомпрометирована злоумышленником, он мог украсть файл

паролей. В подобных обстоятельствах разумно изменить все пароли. В организации должны быть заготовлены процедуры для быстрого и эффективного выполнения такой работы. Конкретный способ действий может зависеть от серьезности проблемы. В случае выявленной атаки, наносящей ущерб, Вы можете принудительно блокировать все счета и присвоить пользователям новые пароли, прежде чем они смогут вновь войти в систему. В некоторых организациях пользователям рассылаются сообщения с просьбой изменить пароль, возможно, с указанием срока исполнения. Если пароль в оговоренное время не меняют, счет блокируется.

Пользователи должны знать стандартные процедуры управления паролями, применяемые при нарушениях режима безопасности. Один из хорошо известных мошеннических приемов, о котором сообщила группа реагирования на нарушения информационной безопасности (Computer Emergency Response Team, CERT), состоит в рассылке пользователям сообщений, вроде бы от имени местного системного администратора, с предложением изменить пароль на новое, сообщаемое тут же, значение [24]. Конечно, сообщения рассылали не администраторы, а злоумышленники, пытающиеся таким образом получить доступ к счетам. Пользователей следует предупредить о необходимости докладывать администраторам обо всех подозрительных запросах, аналогичных упомянутому.

4.4. Процедуры конфигурационного управления

Обычно конфигурационное управление применяют в процессе разработки программного обеспечения. Однако, оно, несомненно, в равной степени применимо и в операционном смысле. Действительно, поскольку многие системные программы предназначены для проведения в жизнь политики безопасности, необходимо иметь уверенность в их корректности. Иными словами, нельзя допускать произвольных изменений системных программ (таких как ОС). Как минимум, процедуры должны определять. кто имеет право изменять системы, при каких обстоятельствах и как эти изменения следует документировать.

В некоторых организациях конфигурационное управление разумно применять и к физическому конфигурированию аппаратуры. Вопросы поддержания правильных и авторизованных аппаратных конфигураций должны получить соответствующее освещение в Вашей политике безопасности.

4.4.1. Нестандартные конфигурации

Иногда полезно внести в конфигурацию небольшие нестандартности, чтобы противостоять "стандартным" атакам, применяемым некоторыми злоумышленниками. В число нестандартных частей может входить оригинальный алгоритм шифрования паролей, необычное расположение конфигурационных файлов, а также переписанные или функционально ограниченные системные команды.

К сожалению, нестандартные конфигурации не свободны от недостатков. Внесение изменений усложняет сопровождение систем, поскольку необходимо написать дополнительную документацию, особым образом устанавливать новые версии программного обеспечения. Обычно в штате организации приходится держать специалиста "по нестандартностям".

Вследствие отмеченных недостатков, нестандартные конфигурации, как правило, используются лишь на экранирующих системах (см. п. 3.9.1). Межсетевые экраны модифицируется нестандартным образом, поскольку они является предполагаемым объектом атак, а конфигурация внутренних систем, расположенных за "противопожарной перегородкой", остается стандартной.

5. Реакция на нарушения безопасности

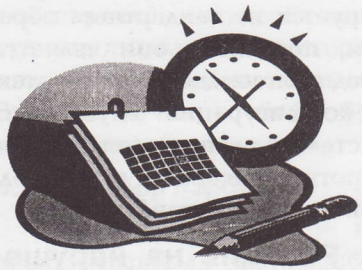
5.1. Обзор

В данной главе излагаются соображения, применимые к ситуациям, когда происходит нарушение информационной безопасности отдельного компьютера, сети, организации или корпоративной среды. Основное положение состоит в том, что враждебные действия, будь то атака внешних злоумышленников или месть обиженного сотрудника, необходимо предусмотреть заранее. Ничто не может заменить предварительно составленного плана восстановительных работ.

Традиционная информационная безопасность, хотя и имеющая весьма важное значение для общеорганизационных защитных планов, как правило, концентрируется вокруг защиты от атак и, до некоторой степени, вокруг их обнаружения. Обычно почти не уделяют внимания мерам, предпринимаемым, когда атака уже идет. В результате поспешных, непродуманных действий могут быть затруднены выявление причины инцидента, сбор улик для расследования, подготовка к восстановлению системы и защита ценной информации.

5.1.1. Имейте план, которому будете следовать во время инцидента

Частью реакции на нарушения безопасности является предварительная подготовка ответных мер. Под этим понимается поддержание должного уровня защиты, так что ущерб даже от серьезного инцидента будет ограниченным. Подготовка



включает в себя составление руководства по мерам реагирования на инциденты и плана восстановительных работ. Наличие отпечатанных планов способно устранить многие двусмысленности, возникающие во время инцидента, и ведет к серии более точных и основательных ответов. Далее, частью защиты является выработка процедуры извещения об инциденте, чтобы каждый знал, кто кому звонит и по каким номерам. Целесообразно устраивать "учебные тревоги", когда сотрудники службы безопасности, системные администраторы и руководители отрабатывают реакцию на инциденты.

Отработка эффективных ответов на инциденты важна по многим причинам. Главнейшая из них — чисто человеческая: предотвращение угрозы жизням людей. Некоторые компьютерные системы критически важны для сохранения жизней (например, системы жизнеобеспечения в больницах или комплексы, участвующие в управлении движением воздушных судов).

Еще одно существенное достоинство предварительной подготовки, о котором часто забывают, носит экономический характер. Содержание технического и управленческого персонала, ответственного за реакцию на инциденты, требует значительных ресурсов, которые с выгодой можно было бы употребить на другие нужды. Если персонал обучен эффективным приемам реагирования, обслуживание инцидентов будет отнимать меньше времени.

Третье достоинство — обеспечение защиты секретной, критически важной или частной информации. Весьма опасно то, что компьютерный инцидент может разрушить невосстановимую информацию. Эффективная реакция на инциденты минимизирует эту опасность. Когда речь идет о секретной информации, следует учесть и включить в план соответствующие правительственные постановления.

Четвертое достоинство касается связей с прессой. Сведения о компьютерном инциденте могут повредить репутации организации среди нынешних или потенциальных клиентов. Эффективная реакция на инцидент уменьшает вероятность нежелательной огласки.

Наконец, упомянем правовой аспект. Можно представить себе ситуацию, когда организация подвергается судебному преследованию, поскольку один из принадлежащих ей узлов был использован для атаки на сеть. С аналогичными проблемами могут столкнуться люди, реализующие заплаты или надстройки, если те оказались неэффективными и не смогли предотвратить ущерб или сами стали причиной ущерба. Знание уязвимых мест операционных систем и типичных приемов атаки, а также принятие превентивных мер поможет избежать конфликтов с законом.

5.1.2. Порядок изложения в данной главе можно использовать в качестве плана

Данная глава организована таким образом, что ее содержание может послужить отправной точкой при написании политики безопасности, касающейся реакции на инциденты. В политике должны быть освещены следующие темы:

- Обзор (цели, преследуемые политикой безопасности в плане реакции на инциденты).
- Оценка (насколько серьезен инцидент).
- Извещение (кого следует известить об инциденте).
- Ответные меры (что следует предпринять в ответ на инцидент).
- Правовой аспект (каковы правовые последствия инцидента).
- Регистрационная документация (что следует фиксировать до, во время и после инцидента).

Каждая из перечисленных тем важна при общем планировании реакции на инциденты. Оставшаяся часть главы посвящена их подробному изложению. Будут сформулированы рекомендации по формированию политики безопасности, касающейся реакции на инциденты.

5.1.3. Возможные цели и побудительные мотивы эффективной реакции на инциденты

Как и во всякой деятельности по планированию, в первую очередь необходимо уяснить преследуемые цели. Эти цели следует упорядочить в порядке убывания важности. Итоговый список, конечно, будет разным для разных организаций. Ниже приведен один из возможных вариантов.

- Гарантировать целостность критических важных (для сохранения человеческих жизней) систем.
- Сохранить и восстановить данные.
- Сохранить и восстановить сервисы.
- Выяснить, почему инцидент стал возможен.
- Предотвратить развитие вторжения и будущие инциденты.
- Избежать нежелательной огласки.
- Найти виновников.
- Наказать нарушителей.

Важно заранее определить приоритеты действий, совершаемых во время инцидента.

Бывают столь сложные случаи, когда невозможно одновременно принять все необходимые ответные меры; без учета приоритетов тут не обойтись. Хотя, как всегда, шкала приоритетов зависит от организации, следующий список может послужить отправной точкой при выработке иерархии ответных мер.

- Первый приоритет — защитить жизнь и здоровье людей; при всех обстоятельствах защита человеческих жизней должна стоять на первом месте.
- Второй приоритет — защитить секретные и/или критически важные данные (в соответствии с правительственными или организационными нормами).
- Третий приоритет — защитить прочие данные, включая частную, научную и управленческую информацию, поскольку потеря данных дорога с точки зрения ресурсов, затраченных на их накопление.
- Четвертый приоритет — предотвратить повреждение систем (потерю и изменение системных файлов, повреждение дисководов и т.п.) чтобы избежать дорогостоящих простоев и восстановлений.
- Пятый приоритет — минимизировать урон, нанесенный вычислительным ресурсам; во многих случаях лучше выключить систему или отсоединить ее от сети, чем подвергать риску информацию, программное обеспечение или аппаратуру.

Важным следствием определения приоритетов является то, что, после человеческих жизней и интересов государственной безопасности, наиболее ценным активом обычно являются данные, а не программное или аппаратное обеспечение. Хотя нежелательны любые потери, системы можно заменить; в то же время потерю или компрометацию данных (особенно секретных), как правило, нельзя допускать ни при каких обстоятельствах.

Как уже отмечалось, частью реакции на инциденты является предварительная подготовка ответных мер. Для каждой машины и системы должна существовать и выполняться процедура резервного копирования. Наличие копий в значительной степени устраняет потери даже после серьезных инцидентов, поскольку исключаются массовые потери данных. Далее, Ваши системы должны иметь безопасную конфигурацию. Под этим понимается устранение слабостей, проведение эффективной политики управления паролями, а также использование других процедур, разъясняемых далее.

5.1.4. Руководство по местной политике безопасности и юридическим положениям

Любой план реагирования на инциденты должен составляться на основе политики безопасности и юридических положений. Правительственные и частные организации, имеющие дело с секретной информацией, должны следовать дополнительным правилам.

Политика, разработанная Вашей организацией применительно к реакции на нарушения режима безопасности (см. разделы 2.4 и 2.5), позволит оформить ответные меры. Например, нет особого смысла создавать механизмы для отслеживания нарушителей, если Ваша организация не собирается после поимки предпринимать против них какие-либо действия. На Ваши планы может влиять политика других организаций. Например, телефонные компании обычно сообщают информацию для прослеживания звонков только правоохранительным органам.

В разделе 5.5 отмечается, что если Вы собираетесь предпринимать правовые акции, необходимо следовать особым рекомендациям, чтобы собранная Вами информация могла быть использована в качестве свидетельских показаний.

5.2. Оценка

5.2.1. А что на самом деле?

На этой фазе точно выясняется характер проблем. Конечно, многие, если не большинство, проявлений, часто приписываемых вирусным инфекциям или вторжениям злоумышленников, являются следствием обычных отклонений, таких как аппаратные сбои. Чтобы понимать, действительно ли имеет место нарушение режима безопасности, полезно приобрести и использовать специальное программное обеспечение. Например, широко доступные программные пакеты могут оказать существенную помощь в выявлении вируса, проникшего в Macintosh. Весьма полезна и регистрационная информация, особенно применительно к сетевым атакам. При подозрениях на вторжение чрезвычайно важно сделать моментальный снимок системы. Многие инциденты порождают целую цепь событий, и снимок системы, сделанный на начальной стадии, может оказаться полезнее других мер для установления сути проблемы и источника опасности. Наконец, важно завести регистрационную книгу. Запись системных событий, телефонных разговоров, временных меток и т.д. способна ускорить и систематизировать процесс идентификации проблемы, послужить основой последующих действий по нейтрализации инцидента.

Имеется ряд отчетливых признаков, или "симптомов" инцидента, заслуживающих особого внимания:

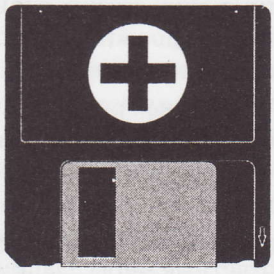
- Крахи системы.
- Появление новых пользовательских счетов (например,

необъяснимым образом создался счет RUMPLESTILTSKIN) или необычайная активность со стороны пользователя (счета), практически не подававшего признаков жизни в течение нескольких месяцев.

- Новые файлы (обычно со странными именами, такими как data.xx или k).
- Рассогласования в учетной информации (например, на UNIX-системах это может проявляться как сокращение файла /usr/admin/lastlog, что вызывает сильные подозрения в присутствии нарушителя).
- Изменения в размерах и датах файлов (например, пользователя MS-DOS должно насторожить внезапное удлинение .EXE-файла более чем на 1800 байт).
- Попытки записи в системные файлы (например, системный администратор замечает, что привилегированный пользователь VMS пытается изменить RIGHTSLIST.DAT).
- Модификация или удаление данных (например, начали исчезать файлы).
- Отказ в обслуживании (например, системные администратор и все остальные пользователи оказались выброшенными из UNIX-системы, которая перешла в однопользовательский режим).
- Необъяснимо низкая производительность системы (например, необычно плохое время отклика системы).
- Аномалии (например, на экране терминала вдруг появляется слово GOTCHA, или раздаются частые и необъяснимые звуковые сигналы).
- Подозрительные пробы (например, многочисленные неудачные попытки входа с другого узла сети).
- Подозрительное рысканье (например, некто стал пользователем root UNIX-систе-

мы и просматривает файл за файлом).

Ни один из этих признаков не может служить бесспорным доказательством нарушения режима безопасности, точно так же, как реальный инцидент обычно не сопровождается всем набором симптомов. Если, однако, Вы заметили какой-либо из перечисленных признаков, следует подозревать нарушение и действовать соответственно. Не существует формулы, позволяющей с абсолютной достоверностью обнаруживать инциденты. Пожалуй, единственным исключением являются антивирусные пакеты. Если они говорят, что вирус есть, им можно верить. В такой ситуа-



ции лучше всего воспользоваться помощью других технических специалистов и сотрудников службы информационной безопасности и сообща решить, действительно ли инцидент имеет место.

5.2.2. Масштабы инцидента

Идентификации инцидента сопутствует выяснение его масштабов и возможных последствий. Для эффективного противодействия важно правильно определить границы инцидента, Кроме того, оценка возможных последствий позволит установить приоритеты при выделении ресурсов для принятия ответных мер. Без выяснения масштабов и возможных последствий события трудно определить, как именно нужно действовать.

Для определения масштабов и возможных последствий, следует воспользоваться набором критериев, подходящих для конкретной организации и имеющихся связей с внешним миром. Вот некоторые из них:

- Затрагивает ли инцидент несколько организаций?
- Затрагивает ли инцидент многие компьютеры Вашей организации?
- Находится ли под угрозой критически важная информация?
- Какова стартовая точка инцидента (сеть, телефонная линия, локальный терминал и т.д.)?
- Знает ли об инциденте пресса?
- Каков потенциальный ущерб от инцидента?
- Каково предполагаемое время ликвидации инцидента?
- Какие ресурсы требуются для ликвидации инцидента?

5.3. Возможные типы извещений

Когда Вы убедились, что нарушение режима безопасности действительно имеет место, следует известить соответствующий персонал. Чтобы удержать события под контролем и с технической, и с эмоциональной точек зрения, очень важно, кто и как будет извещен.

5.3.1. Внятность

Прежде всего, любое извещение, направленное своему или стороннему сотруднику, должно быть внятным. Это значит, что любая фраза об инциденте (идет ли речь об электронном сообщении, телефонном звонке или факсе) обязана быть ясной,

точной и полной. Всякий "туман" в извещении, направленном человеку, от которого Вы ждете помощи, отвлечет его внимание и может повести к недоразумениям. Если предлагается разделение труда, полезно снабдить каждого участника информацией о том, что делают другие. Это не только уменьшит дублирование, но и позволит человеку, занятому определенной работой, знать, где получить дополнительные сведения, чтобы справиться со своей частью проблемы.

5.3.2. Правдивость

Другой важный аспект извещений об инциденте — правдивость. Попытки скрыть отдельные моменты, сообщая ложную или неполную информацию, способны не только помешать принятию эффективных ответных мер; они могут повести даже к ухудшению ситуации. Это тем более верно в случае, когда об инциденте узнали журналисты. Если имеет место достаточно серьезный инцидент, привлекший внимание прессы, то, скорее всего, любая сообщенная Вами ложная информация не получит подтверждения из других источников. Это бросит тень на организацию и испортит отношения с журналистами, а, значит, и с общественностью.

5.3.3. Выбор языка

Язык, которым написано извещение, существенным образом влияет на восприятие информации об инциденте. Если Вы используете эмоциональные обороты, Вы увеличиваете ощущение опасности и ожидание неблагоприятного завершения инцидента. Важно сохранять спокойствие и в письменных, и в устных извещениях.

Другим моментом, связанным с выбором языка, является извещение нетехнического и внешнего персонала. Важно точно описать инцидент, без лишней тревоги и непонятных фраз. Хотя неспециалистам объяснить суть дела труднее, зачастую это более важно. Нетехническое описание может понадобиться для высшего руководства, прессы или сотрудников правоохранительных органов. Важность подобных извещений нельзя недооценивать. От этого зависит, получит ли инцидент адекватное решение или приведет к еще более серьезным последствиям.

5.3.4. Извещение конкретных лиц

Кого извещать во время и после инцидента? На этот предмет можно рассмотреть несколько категорий лиц.

- Персонал в точках контакта (техническая и административная группы, группа реагирования, органы дознания, другие правоохранительные органы, производители, поставщики услуг). Необходимо определить, кто отвечает за извещения в адрес каждой из перечисленных контактных групп.
- Более широкое сообщество (пользователи).
- Другие организации, вовлеченные в инцидент.

Следует заранее установить, кого извещать из центральной точки контакта организации (см. также п. 5.3.6). Список лиц в каждой из выбранных категорий поможет сэкономить массу времени в случае нарушения режима безопасности. В суете инцидента, когда срочные дела накладываются друг на друга, очень трудно выяснять, где и кого можно отыскать.

Кроме лиц, отвечающих за определенные аспекты реакции на инциденты, в извещении нуждаются другие организации, которых нарушение затронуло или может затронуть. Пользователям зачастую также полезно знать об инциденте. Им разумно направить отчет о нарушении (если этот отчет решено сделать открытым).

5.3.5. Связи с общественностью – пресс-релизы

Один из самых важных вопросов — когда, кто и насколько много должен сообщить общественности через прессу. При этом следует учитывать несколько моментов. Во-первых, если в организации существует пресс-центр, важно задействовать именно его. Сотрудники пресс-центра имеют опыт общения с журналистами, и это поможет сохранить лицо организации во время и после инцидента. С сотрудниками пресс-центра можно говорить откровенно, они сами буферизуют предназначенную для прессы информацию, а Вы в это время сможете заниматься инцидентом.

Если пресс-центра нет, следует тщательно взвешивать сообщаемые прессе сведения. Если информация конфиденциальна, разумно ограничиться минимумом данных обзорного характера. Весьма возможно, что все, сообщенное прессе, быстро дойдет до виновника инцидента. С другой стороны, как отмечалось выше, введение прессы в заблуждение может оказаться бумерангом, наносящим больший вред, чем разглашение конфиденциальной информации.

Хотя заранее сложно определить, насколько детальные сведения стоит сообщать прессе, разумно учесть следующие соображения.

- Избегайте технических деталей. Детальная информация об инциденте может повести к повторению подобных нарушений или даже помешать

организации расследовать текущий случай.

- Избегайте предположений. Предположения о виновнике инцидента и его побудительных мотивах могут оказаться ошибочными, что способно усугубить ситуацию.
- Работайте с профессионалами из правоохранительных органов, чтобы обеспечить защиту улик. Если в деле участвуют следственные органы, убедитесь, что собранные улики не стали достоянием прессы.
- Избегайте интервью, если Вы не готовы к ним. Помните, что журналисты попытаются вытянуть из Вас максимум информации, в том числе конфиденциальной.
- Не позволяйте прессе отвлекать Ваше внимание от реакции на инцидент. Постоянно помните, что успешная борьба с нарушением — дело первостепенной важности.

5.3.6. Чьей помощью воспользоваться?

В мире существует довольно много групп реагирования на нарушения информационной безопасности (например, CERT, CIAC). Аналогичные группы имеются во многих важных правительственных агентствах и больших корпорациях. Если у Вашей организации есть контакты с подобной группой, с ней необходимо связаться в первую очередь и как можно раньше. Такие группы отвечают за координацию реакции на инциденты нескольких организаций или более крупных сообществ. Даже если кажется, что нарушение затрагивает только одну организацию, информация, доступная через группу реагирования, способна помочь успешной борьбе с нарушением.

При выработке политики, касающейся реакции на инциденты, может быть принято решение о создании собственной группы реагирования по типу существующих, отвечающей перед организацией за борьбу с нарушениями информационной безопасности. Если группа создана, ей необходимо наладить взаимодействие с аналогичными структурами — во время инцидента налаживать доверительные отношения гораздо труднее.

5.4. Ответные меры

Важная тема, которой мы пока не касались, — это реальные меры, предпринимаемые для борьбы с нарушением. Их можно подразделить на следующие основные категории: сдерживание, ликвидация, восстановление, "разбор полетов".

Сдерживание

Цель сдерживания — ограничить атакуемую область. Например, важно как можно быстрее приостановить распространение червя в сети. Обязательной частью сдерживания является принятие решений (останавливать ли систему, отсоединять ли ее от сети, отслеживать ли ее работу и события в сети, устанавливать ли ловушки, отключать ли некоторые сервисы, такие как удаленная пересылка файлов в ОС UNIX и т.д.). Иногда подобные решения очевидны. Если риску подвергается секретная, конфиденциальная или частная информация, систему нужно остановить. В некоторых случаях стоит пойти на риск, связанный с нанесением системе определенного ущерба, если поддержание ее работы способно помочь в идентификации злоумышленника.

Сдерживание должно выполняться с использованием предварительно выработанных процедур. Ваша организация должна определить приемлемые границы рисков при борьбе с нарушениями и предложить соответствующие стратегические и тактические решения. Наконец, на стадии сдерживания должны извещаться заранее выбранные инстанции.

Ликвидация

После обнаружения инцидента необходимо в первую очередь позаботиться о его сдерживании. Когда эта задача решена, можно приступать к ликвидации. В этом Вам может помочь программное обеспечение. Например, существуют программы, ликвидирующие вирусы в небольших системах. Если нарушитель создал какие-либо файлы, самое время их удалить. В случае вирусной инфекции важно вычистить все диски, содержащие зараженные файлы. Убедитесь в чистоте резервных копий. Многие системы, подвергавшиеся вирусным атакам, время от времени заражаются повторно только потому, что не производится систематическая очистка резервных носителей.

Восстановление

Когда инцидент ликвидирован, наступает время восстановления, то есть приведения системы в нормальное состояние. В случае сетевых атак важно установить заплаты, ликвидирующие использованные системные слабости.

"Разбор полетов"

Одну из самых важных стадий реакции на инциденты, о которой, тем не менее, почти всегда забывают, можно назвать "разбором полетов". Данная стадия важна потому, что она позволяет всем причастным лицам извлечь уроки из инцидента (см. раздел 6.3), чтобы в будущем в аналогичных ситуациях действовать эффек-

тивнее. В процессе "разбора полетов" служба информационной безопасности объясняется перед руководством и систематизирует информацию, необходимую для юридических акций.

Самый важный элемент данной стадии — анализ случившегося. Что именно и когда произошло? Насколько хорошо сработал персонал? Какая срочная информация понадобилась в первую очередь и как ее быстрее всего можно было получить? Что в следующий раз нужно делать по-другому? Постинцидентный отчет ценен как руководство к действию в аналогичных случаях. Составление хронологии событий (с указанием точного времени) важно и с юридической точки зрения. Необходимо также в кратчайшие сроки получить денежную оценку ущерба, нанесенного инцидентом: утраченных программ и файлов, повреждений аппаратуры, потерь времени на восстановление измененных файлов, реконфигурацию атакованных систем и т.п. Эта оценка может послужить основанием для последующего официального расследования.

5.4.1. Единая точка контакта

Когда инцидент в разгаре, важно решить, кто координирует действия множества специалистов. Принципиальной ошибкой была бы организация нескольких точек контакта, которые не в состоянии наладить согласованное управление событиями, а лишь увеличивают общую неразбериху, вызывая своими указаниями напрасную или неэффективную затрату усилий.

Человек, находящийся в единой точке контакта, может быть, а может и не быть руководителем работ по борьбе с нарушением. В принципе речь идет о двух разных ролях, для которых нужно подобрать "исполнителей". Руководитель работ принимает решения (например, он интерпретирует политику безопасности применительно к происходящим событиям). На него возлагается ответственность за реакцию на инцидент. Напротив, непосредственная функция точки контакта состоит в координации усилий всех сторон, вовлеченных в ликвидацию инцидента.

В точке контакта должен находиться специалист, техническая подготовка которого позволяет ему успешно координировать действия системных администраторов и пользователей. Нередко управленческая структура организации такова, что администратор множества ресурсов не имеет достаточной технической подготовки и не знает деталей функционирования компьютеров, но, тем не менее, отвечает за их использование.

Другая важная функция точки контакта — поддержание связей с правоохранительными органами и другими внешними организациями, когда возникает нужда в согласованных действиях нескольких инстанций.

Наконец, если предусматриваются правовые действия, такие как расследование, сотрудник, обслуживающий точку контакта, может представлять организацию в суде. Если свидетелей несколько, их показания трудно координировать, а это ослабляет позиции обвинения и затрудняет наказание нарушителя. Сотрудник точки контакта может представить суду собранные улики, минимизируя тем самым число прочих свидетелей. Как показывает опыт, чем больше свидетелей рассказывает об одном и том же, тем меньше вероятность, что суд им поверит.

5.5. Регистрационная документация

Целесообразно документировать все детали, связанные с инцидентом. В результате Вы получите информацию, незаменимую для восстановления хода событий. Детальное документирование в конечном итоге ведет к экономии времени. Если, например, не зафиксировать телефонный звонок, Вы, скорее всего, забудете почти все, что Вам сообщили. В результате Вам придется звонить еще раз и повторно получать информацию. При этом будет потрачено и Ваше, и чужое время, что едва ли можно считать приемлемым. Фиксация деталей поможет и при проведении расследования. Далее, документирование инцидента позволяет оценить размер нанесенного ущерба (что необходимо и Вашему руководству, и правоохранительным органам) и организовать "разбор полетов", из которого Вы можете извлечь полезные уроки.

Как правило, на ранних стадиях инцидента невозможно определить, понадобится ли расследование, поэтому Вы должны вести документацию так, как будто собираете улики для судебного разбирательства. Необходимо зафиксировать по крайней мере следующее:

- Все системные события (приобщите к документации системный регистрационный журнал).
- Все Ваши действия (с указанием времени).
- Все телефонные переговоры (имя собеседника, дата, время и содержание разговора).

Самый простой способ сохранить документацию — записывать все в регистрационную книгу. Это избавит Вас от поиска среди разрозненных листов бумаги и предоставит в случае необходимости централизованный, упорядоченный по времени источник информации. Большая часть записанных сведений может понадобиться в случае судебного рассмотрения. Таким образом, если Вы начали подозревать, что инцидент приведет к расследованию, или когда рас-

следование уже началось, Вы должны регулярно (например, ежедневно) относить в архив подписанные Вами копии страниц регистрационной книги вместе с другими необходимыми носителями информации, чтобы сохранить их в надежном месте. Разумно потребовать квитанцию о сдаче документации на хранение, с подписью и датой. Если всего этого не сделать, суд может не принять Ваших показаний.

6. Выработка мер, предпринимаемых после нарушения

6.1. Обзор

После ликвидации нарушения режима информационной безопасности, необходимо предпринять ряд действий, а именно:

- Произвести переучет системных активов, то есть тщательно проверить, как инцидент повлиял на состояние систем.
- Уроки, извлеченные из инцидента, должны найти отражение в пересмотренной программе обеспечения безопасности, чтобы не допустить повторения аналогичного нарушения.
- Произвести новый анализ риска с учетом информации, полученной вследствие инцидента.
- Должно быть начато следствие против виновников инцидента, если это признано необходимым.

Перечисленные шаги направлены на обеспечение комитета по политике безопасности предприятия обратной связью, чтобы политика оперативно пересматривалась и подправлялась.

6.2. Устранение слабостей

Устранить все слабости, сделавшие возможным нарушение режима безопасности, весьма непросто. Ключевым моментом здесь является понимание механизма вторжения. В некоторых случаях разумно как можно быстрее отключить доступ ко всей системе или к некоторым из ее функциональных возможностей, а затем поэтапно возвращать ее в нормальное состояние. Учтите, что полное отключение доступа во время инцидента заметят все пользователи, в том числе и предполагаемые виновники; системные администраторы должны помнить об этом. Естественно, ранняя огласка может помешать следствию. Однако, продолжение инцидента порой чревато увеличением ущерба, усугублением ситуации или даже привлечением к административной или уголовной ответственности.

Если установлено, что вторжение стало возможным вследствие дефектов аппаратного или программного обеспечения, следует как можно быстрее уведомить производителя (или поставщика), а также группу реагирования CERT. Настоятельно рекомендуется включить в текст политики безопасности соответствующие телефонные (факсовые) номера, а также адреса электронной почты. Чтобы можно было оперативно уяснить суть проблемы, дефект нужно описать максимально детально (включая информацию о его использовании нарушителем).

После вторжения к системе в целом и к каждому компоненту следует относиться с подозрением. В первую очередь это касается системных программ. Ключевым элементом восстановления скомпрометированной системы является предварительная подготовка. Сюда входит вычисление контрольных сумм для всех лент, полученных от поставщика (желательно, чтобы алгоритм вычисления контрольных сумм был устойчив к попыткам взлома). См. [10], а также пп. 3.9.4.1, 3.9.4.2. Взяв полученные от поставщика ленты, нужно начать анализ всех системных файлов, доводя до сведения всех вовлеченных в ликвидацию инцидента лиц информацию обо всех найденных отклонениях. Порой бывает трудно решить, с какой резервной копии восстанавливаться; помните, что до момента обнаружения инцидент мог продолжаться месяцы или даже годы, и что под подозрением может быть работник предприятия или иное лицо, располагавшее детальным знанием системы или доступом к ней. Во всех случаях предварительная подготовка позволит определить, что можно восстановить. В худшем случае самым благоразумным решением будет переустановка системы с носителей, полученных от поставщика.

Извлекайте уроки из инцидента и всегда корректируйте политику и процедуры безопасности, чтобы отразить изменения, необходимость которых выявил инцидент.

6.2.1. Оценивая ущерб

Прежде чем начинать восстановительные работы, необходимо уяснить истинные размеры ущерба. Возможно, на это уйдет много времени, но зато появится понимание природы инцидента и будет заложена база для проведения расследования. Лучше всего сравнивать текущее состояние с резервными копиями или с лентами, полученными от поставщика; еще раз напомним: предварительная подготовка — ключевой элемент восстановления. Если система поддерживает централизованное ведение регистрационного журнала (как правило, так и бывает), перемещайтесь по журналу назад и отмечайте аномалии. Если ведется учет запускаемых процессов и времени сеансов, попытайтесь определить типичные профили использования системы. В меньшей степени способна пролить свет на ин-

цидент статистика доступа к дискам. Учетная информация может дать богатую пищу для анализа инцидента и официального расследования.

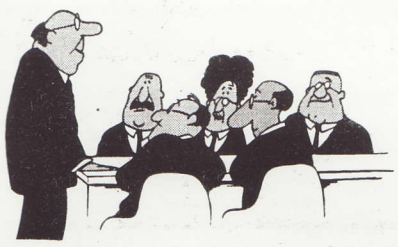
6.2.2. Восстановительные работы

После оценки ущерба следует разработать план восстановительных работ. Как правило, лучше всего восстанавливать сервисы в порядке поступления заявок от пользователей, чтобы минимизировать причиняемые неудобства. Помните, что наличие подходящих процедур восстановления крайне важно; сами эти процедуры специфичны для каждой организации.

Возможно, придется вернуться к начальному состоянию системы с последующей ее настройкой. Чтобы облегчить действия даже в таком, наихудшем, случае, храните записи о начальных установках системы и обо всех внесенных изменениях.

6.2.3. "Разбор полетов"

После того, как система вроде бы приведена в "безопасное" состояние, в ней, возможно, продолжают таиться дыры или даже ловушки. На фазе "разбора полетов" система должна быть тщательно обследована, чтобы выявить проблемы, упущенные при восстановлении. В качестве отправной точки разумно воспользоваться программными средствами обнаружения слабостей конфигурации (такими как COPS). Следует, однако, помнить, что эти средства не заменяют постоянного системного мониторинга и хороших административных процедур.



6.2.4. Ведите журнал безопасности

Как отмечалось в разделе 5.6, журнал безопасности наиболее полезен на этапе устранения уязвимых мест. В этой связи упомянем два момента. Во-первых, следует документировать процедуры, использованные для восстановления режима безопасности. В это число могут войти командные процедуры, предназначенные для периодического запуска с целью проверки надежности системной защиты. Во-вторых, регистрируйте важные системные события. Это может помочь оценить ущерб от инцидента.

6.3. Усвоение уроков

6.3.1. Понимание урока

По завершении инцидента целесообразно составить отчет, в котором описывается инцидент, способы его обнаружения, процедуры исправления ситуации, процедуры мониторинга и усвоенные уроки. Все это способствует ясному пониманию проблемы. Трудно извлечь уроки из инцидента, если его причины не были поняты.

6.3.2. Ресурсы

6.3.2.1. Дополнительные устройства и методы обеспечения безопасности

Безопасность — это динамический, а не статический процесс. Организации зависят от характера доступных в каждый момент времени защитных средств, устройств и методов. Слежение за новинками в области информационной безопасности поможет поставить новейшие технологии на службу интересам предприятия.

6.3.2.2. Хранилище книг, списков, источников информации

Собирайте книги, списки, источники информации и т.п. как руководства и справочники по защите систем. Все время пополняйте свое собрание. Помните, что вместе с изменениями систем меняются методы и проблемы безопасности.

6.3.2.3. Сформируйте подгруппу

Сформируйте подгруппу из числа системных администраторов, которая станет ядром службы информационной безопасности. Наличие подобного коллективного органа позволит проводить обсуждение вопросов безопасности и сопоставление различных точек зрения. Эта подгруппа может также разработать политику безопасности предприятия и периодически совершенствовать комплекс защитных мер.

6.4. Совершенствование политики и процедур

6.4.1. Сформируйте механизмы для изменения политики, процедур и инструментов

Если нарушение режима безопасности стало возможным из-за плохой политики, то пока политика не скорректирована, организация обречена на повторные неприятности. После ликвидации инцидента следует подвергнуть политику и процедуры пересмотру, чтобы очертить круг изменений, необходимых для недопущения аналогичных случаев. Даже если нарушений нет, разумно периодически пересматривать политику и процедуры, поскольку меняется сама современная компьютерная среда.

6.4.2. Процедуры доклада об инцидентах

Необходимо отладить процедуру доклада об инцидентах, чтобы иметь их детальное описание вместе с принятыми мерами. Каждый инцидент должен разбираться подгруппой информационной безопасности предприятия с целью уяснения его сути и выработки предложений по совер-

шенствованию политики и процедур безопасности.

7. Литература

1. Quarterman, J., "The Matrix: Computer Networks and Conferencing Systems Worldwide", Pg. 278, Digital Press, Bedford, MA, 1990.
2. Brand, R., "Coping with the Threat of Computer Security Incidents: A Primer from Prevention through Recovery", 1990.
3. Fites, M., Kratz, P. and A. Brebner, "Control and Security of Computer Information Systems", Computer Science Press, 1989.
4. Johnson, D., and J. Podesta, "Formulating a Company Policy on Access to and Use and Disclosure of Electronic Mail on Company Computer Systems", Available from: The Electronic Mail Association (EMA) 1555 Wilson Blvd, Suite 555, Arlington VA 22209, (703) 522-7111, 22 October 1990.
5. Curry, D., "Improving the Security of Your UNIX System", SRI International Report ITSTD-721-FR-90-21, April 1990.
6. Cheswick, B., "The Design of a Secure Internet Gateway", Proceedings of the Summer Usenix Conference, Anaheim, CA, June 1990.
7. Linn, J., "Privacy Enhancement for Internet Electronic Mail: Part I — Message Encipherment and Authentication Procedures", RFC 1113, IAB Privacy Task Force, August 1989.
8. Kent, S., and J. Linn, "Privacy Enhancement for Internet Electronic Mail: Part II — Certificate-Based Key Management", RFC 1114, IAB Privacy Task Force, August 1989.
9. Linn, J., "Privacy Enhancement for Internet Electronic Mail: Part III — Algorithms, Modes, and Identifiers", RFC 1115, IAB Privacy Task Force, August 1989.
10. Merkle, R., "A Fast Software One Way Hash Function", Journal of Cryptology, Vol. 3, No. 1.
11. Postel, J., "Internet Protocol — DARPA Internet Program Protocol Specification", RFC 791, DARPA, September 1981.
12. Postel, J., "Transmission Control Protocol — DARPA Internet Program Protocol Specification", RFC 793, DARPA, September 1981.
13. Postel, J., "User Datagram Protocol", RFC 768, USC/Information Sciences Institute, 28 August 1980.
14. Mogul, J., "Simple and Flexible Datagram Access Controls for UNIX-based Gateways", Digital Western Research Laboratory Research Report 89/4, March 1989.
15. Bellovin, S., and M. Merritt, "Limitations of the Kerberos Authentication System", Computer Communications Review, October 1990.
16. Pfleeger, C., "Security in Computing", Prentice-Hall, Englewood Cliffs, N.J., 1989.
17. Parker, D., Swope, S., and B. Baker, "Ethical Conflicts: Information and Computer Science, Technology and Business", QED Information Sciences, Inc., Wellesley, MA.
18. Forester, T., and P. Morrison, "Computer Ethics: Tales and Ethical Dilemmas in Computing", MIT Press, Cambridge, MA, 1990.
19. Postel, J., and J. Reynolds, "Telnet Protocol Specification", RFC 854, USC/Information Sciences Institute, May 1983.
20. Postel, J., and J. Reynolds, "File Transfer Protocol", RFC 959, USC/Information Sciences Institute, October 1985.
21. Postel, J., Editor, "IAB Official Protocol Standards", RFC 1200, IAB, April 1991.
22. Internet Activities Board, "Ethics and the Internet", RFC 1087, Internet Activities Board, January 1989.
23. Pethia, R., Crocker, S., and B. Fraser, "Policy Guidelines for the Secure Operation of the Internet", CERT, TIS, CERT, RFC in preparation.
24. Computer Emergency Response Team (CERT/CC), "Unauthorized Password Change Requests", CERT Advisory CA-91:03, April 1991.
25. Computer Emergency Response Team (CERT/CC), "TELNET Breakin Warning", CERT Advisory CA-89:03, August 1989.
26. CCITT, Recommendation X.509, "The Directory: Authentication Framework", Annex C.
27. Farmer, D., and E. Spafford, "The COPS Security Checker System", Proceedings of the Summer 1990 USENIX Conference, Anaheim, CA, Pgs. 165-170, June 1990.

INFO

Информационный бюллетень *Jet Info*

Индекс по каталогу РОСПЕЧАТИ - 32555

Главный редактор: В.А.Галатенко
Технический редактор: С.И.Демочкин

Jet Infosystems

Россия, 103006, Москва,
ул.Краснопролетарская, 6
тел. (095) 972 11 82
(095) 972 13 32
факс (095) 972 07 91
e-mail: JetInfo@jet.msk.su