РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНЫЙ УНИВЕРСИТЕТ
ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Кафедра комплексной защиты информации

Митюшин Дмитрий Алексеевич

Информационные технологии. Администрирование подсистем защиты информации

Тема 4. Сущность администрирования

Вопросы:

1. *Функции, процедуры, объекты и задачи административного управления в информационной системе*
2. *Правила, регламенты и стратегия администрирования в ИС*
3. *Технология управления безопасностью информации и ресурсов в автоматизированной системе*
4. *Программы безопасности верхнего и процедурного уровня*
5. *Процедурный уровень информационной безопасности Основные классы мер процедурного уровня*

Литература

1. Клейменов С.А. Администрирование в информационных системах : учеб. пособие для студ. высш. учеб. заведений / С. А. Клейменов, В. П. Мельников, А. М. Петраков ; под ред. В. П. Мельникова. – М.: Издательский центр «Академия», 2008.– 272 с
2. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие / В. В. Бондарев. - Москва : Издательство МГТУ им. Н. Э. Баума-на, 2016. - 250, [2] с.: ил.

1. Функции, процедуры, объекты и задачи административного управления в информационной системе

Основные конфигурации и модели функционирующих ИС требуют организационной, программной и технической поддержки. Это реализуется через работу системного администратора.

Действия, выполняемые администратором, могут изменяться в зависимости от рабочей среды и приложений, с которыми приходится работать. Но независимо от среды необходимо иметь системную политику и строго следовать ей, а также ознакомить сданной политикой всех пользователей.

Это лишь одна из многих стратегий, которым нужно следовать в работе.

Иногда создаётся впечатление, что основная задача системного администратора заключается в выслушивании упрёков в свой адрес, когда система работает не так, как того ожидают пользователи.

Действительно, когда дела идут нормально, работа над системой кажется чем-то, не заслуживающим особого внимания. И лишь тогда, когда система начинает давать сбои, вспоминают о существовании администратора. Самое лучшее, что можно сделать, – это заранее поработать над системой, чтобы не допустить подобной ситуации.

1. Функции, процедуры, объекты и задачи административного управления в информационной системе

Администратор решает самые разные вопросы. Чаще всего его задача заключается в нахождении компромисса между различными противоречивыми интересами.

Администратор – это пользователь со многими привилегиями. Он разрешает все проблемы, возникающие при работе системы, отвечает за её загрузку и остановку.

Независимо от того, занимаете вы формально должность администратора или совмещаете администрирование с другими делами, вашей основной обязанностью будет поддержка системы и обеспечение бесперебойной работы сервисов.

Несомненно, основной задачей системного администратора является поддержка работы компьютеров. При работе с системой необходимо её запускать и останавливать работу. При этом необходимо проверять, работает ли система, есть ли на дисках свободное место и корректно ли работают необходимые сервисы.

Очевидно, что как только поступит сообщение о том, что система перестала работать, руководство сразу же обратит на это внимание.

1. Функции, процедуры, объекты и задачи административного управления в информационной системе

На примере мониторинга, применяемого в системах Unix, можно выделить упреждающие технологии.

Процедура сбора данных или сбор нужной информации по следующим частям информационных СУ:

- центральный процессор (ЦП) – здесь фиксируется использование ЦП, обычно по средней нагрузке, и определяется производительность системы;
- память – сбор данных для её мониторинга осуществляется перемещением на жёсткий диск блоков памяти (страниц памяти), в том числе и блоков с оперативной памятью, и, наоборот, восстановлением в оперативной памяти страниц, хранящихся на диске. При интенсивном обмене информацией между памятью и диском происходит «пробуксовывание» системы;
- файлы журналов – они служат документальным подтверждением ошибок и отказов сервисов, работающих в системе;
- диски – на них хранятся файлы операционных систем (ОС) и БД. Команды ОС прежде всего задействуются с дисков;
- пользователи – их мониторинг распространяется как на авторизованных регистрацией пользователей, так и на законных. Обе эти группы могут быть источниками проблем, возникающих при функционировании системы.

1. Функции, процедуры, объекты и задачи административного управления в информационной системе

В сетевой среде для получения информации о других системах можно воспользоваться возможностями сети, например, с помощью удалённого управления. Чтобы в каждой системе не регистрироваться и не запускать команды, целесообразно пользоваться локальными агентами. Тогда можно выполнять мониторинг какого-либо параметра системы и передавать на удалённую консоль отчёты о его состоянии.

При мониторинге сетевых сервисов можно написать сценарий для одной системы сети, имеющей доступ к сетевым сервисам другой системы, и из центрального пункта осуществлять проверку и сбор данных.

Типовая технология мониторинга (сбор и анализ данных) состояния системы предусматривает четыре этапа:

1) определение цели сбора информации (например, по состоянию обработки сообщений электронной почты, обработки учётных записей зарегистрированных в системе пользователей, реализации соглашений по обслуживанию и т.д.). Здесь же вырабатываются критерии оценки для последующего анализа;
2) создание сценария сбора информации. Необходимо определить последовательность команд, их кратность использования, в том числе и в автоматизированных режимах;
3) систематизация и подготовительная обработка информации – наиболее

1. Функции, процедуры, объекты и задачи административного управления в информационной системе

4) анализ и синтез полученных результатов; определение тенденций и закономерностей реакций системы на воздействие; выявление информации для дальнейшего планирования и принятия решений по системе.

Большое значение в мониторинге ИС придаётся состоянию функционирования системы памяти.

Все команды выполняются программами, записанными на диск (или встроенными в оболочку). В системе Unix все устройства представляются как файлы. Данные, обрабатываемые на узле, также расположены на диске. На диске (в области подкачки) могут быть расположены даже некоторые фрагменты оперативной памяти.

Практически все, с чем работает система, записывается на диск, поэтому нужно вовремя подключать новые диски, создавать разделы файловой системы, проверять целостность файловых систем (в этом поможет команда fsck), создавать резервные копии и восстанавливать данные, а также при необходимости освобождать дисковое пространство.

Необходимо выработать политику резервного копирования. Эта задача часто осложняется тем, что размеры современных дисков очень велики. Производители накопителей на лентах быстро увеличивают объем своих

1. Функции, процедуры, объекты и задачи административного управления в информационной системе

Мониторинг периферийных устройств также необходим. Принтеры, устройства чтения компакт-дисков и другие устройства обычно хорошо работают в среде Unix, однако для этого надо выполнить соответствующие настройки.

Unix представляет все устройства как файлы, поэтому приходится создавать новые записи обустройствах в каталоге /dev.

Unix предоставляет возможность совместного использования принтеров через сеть, однако для этого нужно настроить программу *lp* или *lpr* так, чтобы она отправляла по сети запросы к соответствующей машине. Если принтер подключён к системе, то необходимо сконфигурировать средства, предназначенные для приёма по сети запросов на печать. Также нужно проследить, чтобы в системе спулинга было достаточно дисковой памяти для хранения требуемого количества документов определённого размера.

Нехватка свободного места на диске является основной проблемой при работе с принтерами через сеть.

1. Функции, процедуры, объекты и задачи административного управления в информационной системе

Мониторинг сети – довольно сложная задача.

Большинство систем, работающих под управлением Unix, соединены с другими системами. Это значит, что нужно правильно сконфигурировать каждую систему в сети, чтобы обеспечить взаимодействие между ними.

Способность к обмену информацией не должна снижаться при расширении сети и замене маршрутизаторов, концентраторов, коммутаторов и мостов. Необходимо гарантировать нормальную работу сетевых кабелей, а также обеспечивать нормальное время отклика при повышенной загруженности сети.

Устанавливая новые системы, надо подключить их к сети. В круг обязанностей администратора входит присвоение узлам имён и IP-адресов и настройка сетевых интерфейсов.

После того как новая система будет настроена, необходимо, чтобы о её существовании узнали все остальные системы в сети. Для этого требуется настроить NIS (Network Information Service – служба сетевой информации) или DNS (Domain Name Service – служба доменных имён).

1. Функции, процедуры, объекты и задачи административного управления в информационной системе

Пользователи в мониторинге системы занимают особое положение. Многие системные администраторы жалуются на своих пользователей, хотя именно ради них существуют системы, которыми управляют администраторы. Им часто приходится добавлять и удалять пользователей, следить, чтобы пользователи выполняли корректные действия. Многие задачи, касающиеся работы с пользователями, имеют непосредственное отношение к системе безопасности Unix.

Возможно, придётся изменять пароли пользователей, назначать исходные пароли и следить, чтобы при выборе пароля пользователи не выбирали очень простые последовательности символов.

При этом может пригодиться программа COPS (Computer Oracle and Password System).
Возможно, администратору придётся помогать пользователям решать повседневные задачи, связанные с вычислениями. Если это занимает слишком много времени, то можно придумать другой способ содействия пользователям, например, создать Web-страницу, содержащую список часто встречающихся вопросов и ответы на них (список FAQ), и разместить её во внутренней сети компании.

Большинство разработчиков очень требовательны. Им необходимо

1. Функции, процедуры, объекты и задачи административного управления в информационной системе

Чтобы облегчить эту работу, можно установить систему, с помощью которой пользователь будет сам создавать резервные копии.

Также можно выделить для разработчика определённую область, где он будет иметь право сам устанавливать ПО.

Операционная система в мониторинге – предмет особого внимания администратора. Занимаясь администрированием, приходится часто устанавливать заплаты для компонентов операционной системы или её более новые версии. Это особенно важно при взаимодействии с Интернетом или при работе над проектами, для которых требуются последние версии JVM (JavaVirtual Machine – виртуальная машина Java). Иногда требуется установить заплату (patch), а иногда приходится полностью переустановить систему.

Производители Unix постоянно добавляют новые компоненты к своим операционным системам и устраняют замеченные ошибки.

Обеспечение безопасности системы – ещё одна задача, при решении которой часто приходится устанавливать заплаты в системе. Как правило, очередные пробелы в системе защиты обнаруживаются раз в месяц. В некоторых ОС, не принадлежащих к семейству Unix, такие недостатки выявляются каждую неделю.

1. Функции, процедуры, объекты и задачи административного управления в информационной системе

Доработка ОС может сводиться к замене исполняемого файла, но иногда предполагает достаточно сложные действия, например, изменение двоичного кода ядра с помощью отладчика. Большинство производителей Unix поставляют специальные инструменты, с помощью которых можно быстро и надёжно установить заплаты. Перед изменением ядра Unix всегда нужно создавать резервную копию системы. Также обязательно нужно прочитать файлы readme или инструкцию, поставляемую вместе с заплатами.

Системный администратор должен обновлять ПО и управлять его использованием. В некоторых случаях необходимо убедиться, что все нужные домены запущены и пользователи имеют доступ к требуемым приложениям. Не исключено, что именно в тот момент, когда все приложения заработают нормально, необходимо будет обновить их для того, чтобы они соответствовали новой версии ОС.

Несмотря на то, что вопросы безопасности, как правило, связаны с работой пользователей, необходимо учитывать, что среди них могут быть такие, которые хотят получить доступ к системе, не имея на это права.

Необходимо постоянно принимать меры против несанкционированного доступа; это особенно важно, если система подключена к Интернету. Даже если хакер, проникая в систему, не ставит целью разрушить её, он все равно может случайно

1. Функции, процедуры, объекты и задачи административного управления в информационной системе

Необходимо также проверять защиту каждый день, чтобы узнать, не предпринималась ли попытка взлома. Помогут в этом системы обнаружения вторжений.

Основная задача большинства систем Unix заключается в предоставлении тех или иных сервисов. Система может выполнять функции сервера баз данных, Web-сервера, файлового сервера, почтового сервера и т. д. Главная задача администратора заключается в обеспечении такого уровня обслуживания, который позволит пользователям выполнять свою работу.

От системы постоянно ожидают определённых сервисов. Для того чтобы эффективно обеспечивать сервис, необходимо знать, в чём действительно нуждаются пользователи. Нужно работать, тесно сотрудничая с пользователями, чтобы понимать и удовлетворять их потребности.

Не обязательно дожидаться, когда пользователи обратятся с просьбами и вопросами. Необходимо выступать инициатором взаимодействия с пользователями.

Когда администрация отказывается выделять деньги на покупку оборудования, которое требуют пользователи, считается, что виноват в этом системный администратор. Пользователи часто не отдают себе отчёт, что он работает в

1. Функции, процедуры, объекты и задачи административного управления в информационной системе

Соглашение о предоставляемых услугах – один из способов убедиться в том, что стороны «говорят на одном языке». Достигнув необходимого уровня обслуживания, необходимо контролировать его.

Требуется проверить, имеют ли пользователи доступ к требующимся им данным, хватает ли им времени, выделенного для работы с сетью, чтобы успешно решать повседневные задачи.

Например, система Unix обеспечивает следующие сервисы:

- файлы. Файловый сервер часто использует NFS (Network File System – сетевая файловая система) и предоставляет дисковое пространство и данные компании для совместного использования. В сочетании с резервным копированием это помогает сохранить целостность данных компании и обеспечивает доступ из различных систем. Другой способ работы с файлами – использование протокола System Message Block (SMB), применяющегося в системе Windows;
- принтеры. В настоящее время компьютеры выводят больше бумажных копий данных, чем когда-либо раньше. Некоторые пользователи распечатывают все приходящие к ним письма и подшивают их. Хотя о рациональности таких действий можно поспорить, все равно следует признать, что это отличный способ создания резервных копий;

1. Функции, процедуры, объекты и задачи административного управления в информационной системе

- приложения. Система Unix может служить хорошей базой для работы приложений. В стандартной среде сервера приложений пользователи сначала регистрируются, а затем запускают программу, например, СУБД. С появлением Java и других похожих технологий термин «сервер приложений» приобрёл новый смысл. Система Unix может служить центральным хранилищем для приложений, написанных на Java и представленных в виде файлов .class (скомпилированные Java-программы) и архивов JAR (Java Archive), которые копируются на клиент-машину, например ПК;
- данные. В наше время пользователей часто даже не интересует, какие приложения они используют. Они просто обращаются к данным. Очень важно обеспечить безопасность и целостность данных. В их распоряжении могут оказаться серверы, собирающие данные и преобразующие их в другой формат; такие серверы называются серверами данных;
- Web-документы. Unix очень часто используется для публикации Web-страниц. На работу Web-сервера влияет производительность сети и файловой системы. Если Web-сервер доступен из Интернета, то вопросы защиты приобретают особое значение.

Сервисы, предоставляемые системой, вероятно, будут сочетанием перечисленных ранее типов сервиса. Например, сервер данных может также выполнять функции Web-сервера. Такая система преобразует данные и представляет их в формате Web-документа.

1. Функции, процедуры, объекты и задачи административного управления в информационной системе

Среда Web очень похожа на среду разработки ПО тем, что они обе нуждаются в хранении различных версий документов. Как для HTML и других Web-документов, так и для исходных кодов программ следует обеспечить средства управление версиями. Средства, обеспечивающие контроль за новыми реализациями программ, хорошо работают и с Web-документами. Некоторые подобные пакеты работают в Unix; среди них можно отметить систему SCCS (Source Code Control System – система управления исходными кодами), которая поставляется с многими версиями Unix, и свободно распространяемый продукт RCS (Revision Control System – система управления реализациями).

Помимо нагрузки сервисов, работу которых администратору необходимо обеспечивать, может быть нагрузка по объёму работы.

Администрирование 10 систем Unix в корне отличается от администрирования 1 000 систем, а обслуживать пять пользователей гораздо проще, чем обслуживать 5 000 пользователей.
Каждый узел чем-то отличается от остальных. Особенности работы администратора зависят от перечня сервисов, объёма ресурсов (данных, пользователей, транзакций и т.д.) и типа рабочей среды.
Для того чтобы успешно справиться с ролью администратора, необходимо хорошо знать систему и её отличие от других систем.

2. Правила, регламенты и стратегия администрирования в ИС

2.1. Основные положения стратегии администрирования

Для реализации основных задач ИС администрирование обязано организовать, структурировать и систематизировать обслуживание пользователей. Учитывая декларативный принцип любой системной организации управления, вся стратегия администрирования должна быть первоначально построена на основе правил и регламентов.

Документально оформленные, доведённые до сведения всех сотрудников правила и регламенты необходимы для нормального функционирования любой организации.

Они должны быть соответствующим образом оформлены, утверждены руководством и проверены юристами. Лучше это сделать до того, как возникнет необходимость обращения к подобным документам для решения какой-нибудь острой проблемы. Желательно, чтобы в каждой организации были следующие документы:

- правила административного обслуживания;
- регламенты прав и обязанностей пользователей;
- правила для администраторов (пользователей с особыми привилегиями);
- правила создания «гостевых» учётных записей.

Для систематизации практического опыта можно использовать различные

2. Правила, регламенты и стратегия администрирования в ИС

2.1. Основные положения стратегии администрирования

Преимущества, получаемые при использовании регламентов:

- рутинные задачи всегда выполняются одинаково;
- уменьшается вероятность появления ошибок;
- работа по инструкциям выполняется администратором гораздо быстрее;
- изменения самодокументируются;
- корректность действий администратора можно соизмерять с неким эталоном.

В современных системах почти все стандартные задачи документированы в форме контрольных списков и инструкций. В Unix они называются «run books» или «checklists» и доступны в оперативном режиме или хранятся в печатном виде.

Написанием и поддержкой этих инструкций занимается дополнительная группа системных администраторов (не входящая в состав основного штата системных администраторов, обслуживающих технику и использующих эти инструкции). Тем не менее такая организация и стандартизация в конечном счёте окупаются.

2. Правила, регламенты и стратегия администрирования в ИС

2.1. Основные положения стратегии администрирования

В перечень таких регламентов входят:

- подключения компьютера;
- подключения пользователя;
- настройки и конфигурирования компьютера;
- установки библиотеки TCP-оболочек на компьютер;
- настройки резервного копирования для нового компьютера;
- защита нового компьютера;
- перезапуск сложного программного обеспечения;
- восстановления Web-серверов, которые не отвечают на запросы или не предоставляют данных;
- разгрузки очереди и перезагрузки принтера;
- модернизации операционной системы;
- инсталляции пакета прикладных программ;
- инсталляции программного обеспечения по сети;
- модернизации наиболее важных программ (sendmail, gcc, named и т.д.);
- резервные копирования и восстановления файлов;
- выполнение аварийной остановки системы (всех компьютеров; всех, кроме наиболее важных, компьютеров и т.д.).

2. Правила, регламенты и стратегия администрирования в ИС

2.1. Основные положения стратегии администрирования

Некоторые положения инструкций диктуются особенностями ПО, с которым вы работаете, либо правилами, принятыми в тех или иных сторонних группах, например, у поставщиков услуг Интернета. Соблюдение некоторых положений является обязательным, особенно если вы должны обеспечить секретность данных пользователей. В частности, управление интернет-адресами, именами компьютеров, идентификаторами пользователей и групп, регистрационными именами должно осуществляться единообразно для всех компьютеров организации. Для больших структур (в частности, транснациональных корпораций) такой подход реализовать не просто, но, если удастся это сделать, управление значительно упростится.

Средства, которые облегчают управление хостами и пользовательскими учётными записями, можно получить по сети, например, программы на узле ftp.xor.com. Также ни в коем случае нельзя предоставлять нескольким пользователям одно и то же регистрационное имя. Это правило гораздо легче внедрить, если сразу же устранить соблазн коллективного использования имени. Хорошая альтернатива несанкционированному применению одного и того же имени – «гостевой» компьютер с либеральными правилами создания учётных записей. Однако сейчас, когда некоторые службы (Яндекс, Hotmail, Yahoo и др.) предоставляют адреса электронной почты и существует доступ к Интернету из библиотек, интернет-кафе, такой метод не эффективен.

2. Правила, регламенты и стратегия администрирования в ИС

2.1. Основные положения стратегии администрирования

Многие вопросы регламента относятся не только к локальной административной группе, например:

- нарушения системы защиты;
- управление экспортом в NFS;
- критерии выбора паролей;
- удаление регистрационных имён;
- защита материалов знаком авторского права (например, для файлов MP3 и DVD);
- программное пиратство.

Обеспечение связи между административными группами в крупных организациях – один из важнейших факторов предотвращения проблем и создания атмосферы доверия и сотрудничества.

Некоторые группы администраторов применяют для общения такие средства, как MUD. При разумном использовании, безусловно, будут полезны и другие методы, особенно если часть персонала работает дома.

2. Правила, регламенты и стратегия администрирования в ИС

2.2. Правила и регламенты администрирования

В правилах для администраторов (и других лиц с особым статусом) должны быть сформулированы руководящие принципы использования предоставленных привилегий и соблюдения секретности пользовательских данных. Трудно, конечно, ответить на жалобу пользователя о том, что почта не работает, не видя «отскочивших» сообщений, но копии заголовка в большинстве случаев хватает для определения сути проблемы и способа её устранения.

В системе Unix, например, применяют следующие правила. Если для доступа в систему с правами root применяется программа типа sudo, то администраторам следует выбирать надёжные пароли и не делить учётные записи с кем попало. Регулярно проверяйте пароли системных администраторов при помощи программы crack. Кроме того, важно, чтобы они не использовали команду sudo tcsh, поскольку нарушится способность sudo регистрировать события и выполняемые команды.

Некоторые системные администраторы злоупотребляют своими возможностями. Таким сотрудникам лучше предложить другие должности.

В ряде организаций обладание паролём root является символом занимаемого положения. Иногда этот пароль есть у инженеров, которым он не нужен или не должен выдаваться.

2. Правила, регламенты и стратегия администрирования в ИС

2.2. Правила и регламенты администрирования

Другой проверенный метод – поместить пароль root в конверты спрятать его в известном месте. Администраторы обычно пользуются в своей работе программой sudo; если по какой-либо причине им понадобится пароль root, то они вскроют конверт. После этого пароль root меняется и прячется в новый конверт. Конечно, вскрыть конверт ничего не стоит, но доступ к тому месту, где он хранится, имеют только администраторы.

Большое значение имеют правила и регламенты, которые необходимы в экстренных случаях. Для этого необходимо заблаговременно решить вопрос о том, кто будет руководить работой в случае нарушения защиты. Заранее определяется субординация; имена и телефоны должностных лиц держатся вне системы. Может оказаться так, что лучшим руководителем в подобной ситуации будет администратор сети, а не директор вычислительного центра (обычно он не подходит для этой роли).

Для общения и получения документов обычно пользуются сетью. В случае инцидента с защитой доступ к сетевым средствам может быть затруднён или вообще окажется невозможным. Сведения о своих связях и методиках держатся также вне сети. Нельзя забывать о том, где можно взять последние дамп-ленты и какие команды нужное использовать для восстановления без обращения к файлу /etc/dumpdates. Нужно избегать расспросов со стороны представителей

2. Правила, регламенты и стратегия администрирования в ИС

2.2. Правила и регламенты администрирования

У хакеров в настоящее время распространено взламывание Web-узлов. Для системных администраторов компании, предоставляющей услуги Web-хостинга, такой взлом – очень большая неприятность. Тут же начинаются телефонные звонки от обеспокоенных клиентов, средств массовой информации (СМИ) и партнёров компании. Кто будет отвечать на все эти звонки? Что он скажет? Кто возьмёт на себя ответственность за исправление ситуации? Какими будут обязанности каждого из членов персонала? Если ваш бизнес на виду у широкой общественности, то все это нужно очень тщательно продумать и, возможно, провести учения.

Правила работы по администрированию в аварийных ситуациях требуют чёткого планирования действий всего персонала организации. Действия персонала в случае аварии нужно планировать заранее.

Наиболее сложные аварии случаются на ноутбуках руководителей.

Приведём несколько типовых аварий и непредвиденных ситуаций:

- нарушение защиты (60 % нарушений защиты обычно происходит внутри организации);
- внешние воздействия на технику: скачки напряжения и отключение питания, поломки кондиционеров и вентиляторов, потопы, ураганы, землетрясения,

2. Правила, регламенты и стратегия администрирования в ИС

2.2. Правила и регламенты администрирования

- человеческие ошибки: удалённые или повреждённые файлы и базы данных, потерянная конфигурационная информация (возможно, ваша система зеркалирования данных работает с такой скоростью, что ошибка успевает распространится в ней до того, как вы сообразите, что произошло);
- неожиданный выход из строя аппаратного обеспечения: отказ сервера, поломка жёсткого диска, нарушение работы сети.

В любой из этих ситуаций необходим доступ к копиям важной информации, хранящейся в компьютерах и на внешних носителях.

Для оперативного доступа к таким копиям нужно использовать независимый компьютер с богатым набором всевозможных утилит и инструментальных средств, специально настроенный и оборудованный для использования системными администраторами.

На нем должен работать собственный сервер имён, должен быть полный файл /etc/hosts. Все необходимые для его работы файлы должны храниться на нем, а не где-то в сети. К нему должен быть непосредственно подключён принтер и т.д.

2. Правила, регламенты и стратегия администрирования в ИС

2.2. Правила и регламенты администрирования

На резервной машине следует хранить и иметь под рукой в распечатанном виде следующие данные:

- план действий персонала в случае аварии, в котором должно быть указано, кого и когда оповещать и что говорить;
- номера телефонов обслуживающих организаций и клиентов;
- важнейшие номера телефонов (персонала, полиции, пожарной службы, начальника, агентства по трудоустройству);
- сведения об аппаратном обеспечении и конфигурации программного обеспечения: таблицы разделов дисков, аппаратные установки компьютеров, номера прерываний, номера каналов DMA и т.д.;
- ленты с резервными копиями и расписание резервного копирования, использовавшееся для их создания;
- карты сети;
- серийные номера программного обеспечения, лицензионные данные и пароли;
- контактная информация производителей или продавцов дисков, которые должны быть восстановлены немедленно.

2. Правила, регламенты и стратегия администрирования в ИС

2.2. Правила и регламенты администрирования

При составлении плана аварийных мероприятий обычно предполагается, что административный персонал будет на месте и он в состоянии справиться с ситуацией. Однако в реальности люди болеют, переходят на другие должности, уходят в отпуск и увольняются. Поэтому стоит заранее продумать, где можно быстро найти дополнительный персонал. (Если система не очень устойчива, а персонал неопытен, то недостаточное количество администраторов уже само по себе рискованно.)

Одним из решений может быть договор с местной консультационной компанией или другой организацией, в которой всегда имеются свободные системные администраторы. Но самое главное – обеспечение надёжной работы системы; при необходимости нужно нанять достаточное число администраторов.

План аварийных мероприятий лучше проверить заранее. Необходимо основательно готовиться к выживанию в случае аварии. Возможно, стоит оставить кое-что из запасов, например, фонари с аккумуляторами (есть очень удобные фонари – они вставляются розетку и зажигаются, когда отключается электричество, так что их сразу легко найти).

2. Правила, регламенты и стратегия администрирования в ИС

2.2. Правила и регламенты администрирования

Необходимо также проверить генераторы и источники бесперебойного питания (ИБП), убедиться, что все важные устройства подключены к ИБП, их батареи в порядке и механизм включения питания работает. Для проверки ИБП достаточно вынуть вилку из розетки, а для того, чтобы проверить, все ли важное оборудование к ним подключено, нужно отключить питание в здании или в комнате и убедиться, что все работает.

Как правило, электричество отключается ненадолго, но на всякий случай батареи должны обеспечивать 2 ч работы, чтобы было время правильно выключить технику. Некоторые ИБП оборудованы последовательными портами или интерфейсом Ethernet, позволяющим отключать не самые важные машины через 5 мин после отключения питания (тайм-аут настраивается).

Даже из краткосрочного отключения питания можно извлечь некоторую пользу, например, добавить на сервер ещё один диск или выполнить какую-то пятиминутную работу, которую вы давно запланировали. Некоторые неудобства будут приняты как нечто само собой разумеющееся. Люди обычно спокойнее воспринимают дополнительную пятиминутную задержку после отключения электричества, чем пятиминутное плановое отключение системы, о котором их оповестили за неделю. Если есть старые машины, которыми уже никто не пользуется, не включайте их, пока кто-нибудь не пожалуется на их отсутствие.

2. Правила, регламенты и стратегия администрирования в ИС

2.2. Правила и регламенты администрирования

Системы охлаждения часто оборудованы датчиками температуры со средствами оповещения о её повышении. Лучше задать такую верхнюю границу температуры, чтобы после сигнала хватило времени выключить технику, прежде чем она перегреется и выйдет из строя. Хорошо хранить в машинной комнате обычный термометр или термометр, работающий от батареи. Нужно иметь ввиду, что, как только отключится питание, все электронные индикаторы окажутся бесполезными.

Особенно опасно воздействие непредвиденных обстоятельств: резкое возрастание трафика, ошибки администраторов и т.д. Например, когда провайдеры услуг Интернета объединяются в более крупные компании или приобретаются крупными компаниями, нарушаются их тщательно разработанные планы поддержания избыточных подключений к Интернету. Объединяясь, компании часто объединяют и свои сети. Поэтому может оказаться, что имеющиеся два независимых соединения с Интернетом теперь выходят на общий оптоволоконный кабель.

Когда CNN или Sladshot объявляет, что Web-узел отключён, пользователи могут ринуться смотреть, как дела, в результате чего трафик возрастёт настолько, что может разрушить то, что только что было отремонтировано. Если Web-узел не рассчитан на 25%-е увеличение трафика, то целесообразно использовать

Оно может просто направлять лишние обращения на сервер, возвращающий одну и ту же страницу: «Извините, узел слишком загружен и в данный момент мы не можем обработать ваш запрос».

Другой способ – использование программы tripwire для согласования действий системных администраторов, особенно если разные группы администраторов отвечают за разные аспекты работы одной машины.

Например, заплаты СУБД Oracle и заплаты операционной системы могут конфликтовать друг с другом, и поставившая одну из них группа администраторов может даже не подозревать, что причиной проблемы являются действия второй группы. Сведения, собранные программой tripwire, могут очень пригодиться и организации, предоставляющей административные услуги, если её специалистам нужно восстановить систему клиента после неудачных действий его собственных администраторов.

Эта программа легко определяет, что и когда изменилось, и поможет доказать местным системным администраторам, что именно их действия явились причиной неполадок.

2. Правила, регламенты и стратегия администрирования в ИС

2.3. Особенности реализации технологий администрирования в ИС

Системные администраторы обычно не отвечают за то, что пользователи хранят на машинах, которые они обслуживают. Провайдеры услуг Интернета чаше всего просто направляют всех, кто к ним подключается, к своим клиентам. Вся ответственность за действия клиентов возлагается на самих клиентов, а не на провайдеров или организации, предоставляющие услуги провайдерам.

Целью такой политики является защита провайдеров от ответственности за spam и прочие неприятности, такие как хранение пользователями на своих узлах запрещённых материалов. Необходимо знать соответствующие законодательные акты.

Полезная юридическая информация имеется на узле www.mibh.net. Там есть сведения о незаконных действиях, нарушениях интеллектуальной собственности и нарушениях правил использования продуктов и услуг. Вы найдёте на этом узле список запрещённых действий, ограничений, описание процедур регистрации жалоб и кое-что об ответственности.

2. Правила, регламенты и стратегия администрирования в ИС

2.3. Особенности реализации технологий администрирования в ИС

В то же время существует угроза конфиденциальности, которую представляют провайдеры услуг Интернета. За обеспечение и регулирование конфиденциальности работы в Интернете взялась компания Predictive Networks, которая с помощью провайдеров планирует наблюдать за работой в сети и собирать информацию о посещаемых пользователями URL, ключевых словах, вводимых в программы поиска ресурсов, и т.д. На основе этой информации она будет формировать цифровую подпись и пользовательский профиль, а также использовать его для того, чтобы подбирать интернет-ресурсы и рекламу персонально для пользователя.

Компания Predictive Networks утверждает, что эта информация будет анонимной и можно доверять всем, кто вовлечён в процесс её сбора: сотрудникам компании Predictive Networks, сотрудникам своего интернет-провайдера, а также тем, кто размещает рекламу и ресурсы. Можно запросить копию своей цифровой подписи, но за это придётся заплатить, а также отказаться от использования этого «сервиса», но тогда подключение к Интернету будет стоить дороже или провайдер даже сможет расторгнуть с пользователем договор.

Информацию по этому вопросу можно посмотреть на Web-узле компании Predictive Networks (www.predictivenetworks.com), а также в статье из «PRIVACY Forum Digest» (V09, #13, www.vortex.com).

2. Правила, регламенты и стратегия администрирования в ИС

2.3. Особенности реализации технологий администрирования в ИС

Применение для целей анализа информации и администрирования файлов регистрации является необходимым приёмом. При этом целесообразно использовать для защиты официально заверенные бумажные документы, так как документы, представленные в электронной форме, не всегда могут возыметь должное действие.

Некоторую пользу могут принести штампы времени в файлах регистрации, однако только в том случае, если на компьютере работает Network Time Protocol (NTP), синхронизирующий его часы с реальным временем. Правила безопасности помогут обнаружить злоупотребления.

Несанкционированное использование компьютерных систем фирмы связано с нарушением не только правил фирмы, но и законов государства. Несанкционированное использование является преступлением, влечёт за собой уголовную и гражданскую ответственность и подлежит наказанию, предусмотренному законодательством.

Также рекомендуется помещать в файл /etc/motd (сообщение дня) предупреждение о действующих правилах. Оно может выглядеть следующим образом:

В случае реального или предполагаемого инцидента с системой защиты

2. Правила, регламенты и стратегия администрирования в ИС

2.3. Особенности реализации технологий администрирования в ИС

Для некоторых типов соединений сообщение дня не отображается (например, во время сеанса ftp). Пользователи могут также воспрепятствовать выводу этого сообщения на экран, создав в своих начальных каталогах файл .hushlogin. Можно сделать так, чтобы пользователи прочли это уведомление хотя бы один раз – для этого нужно включить его в файлы запуска, выдаваемые новым пользователям.

Необходимо обязательно указать, что сам факт использования учётных записей пользователей равносилен согласию соблюдать установленные правила. Нужно объяснить, где можно получить экземпляры правил, и поместить основные документы на соответствующей доске объявлений, провести особые меры, которые будут приняты в случае их несоблюдения.

Проблемы в администрировании возникают и при защите авторских прав. Они появляются, например, при использовании возможностей службы Napster при применении формата DVD для просмотра фильмов и проигрывания музыки и в других случаях.

Содержимое диска в формате DVD шифруется по технологии CSS (Content Scrambling System). Это делается для того, чтобы диски могли проигрываться только лицензированными и одобренными плеерами. Эти плееры, как и лицензированное ПО для проигрывания, имеют ключ для раскодирования

2. Правила, регламенты и стратегия администрирования в ИС

2.3. Особенности реализации технологий администрирования в ИС

Надо учитывать, что есть и другие случаи информационного противоборства, уже имеющие системный характер. Так, компания CyberPatrol разработала ПО для фильтрации данных, получаемых из Интернета. Религиозные организации распространяют это программное обеспечение в семьях, имеющих детей, в школах и библиотеках, чтобы оградить детей от того, чего им видеть ненужно. Компания A Canadian and a Swede разработала программу cphack, позволяющую расшифровывать списки блокировки, создаваемые ПО CyberPatrol. Целью этой разработки была необходимость узнать, какие Web-узлы заблокированы, каков уровень ошибок и какие невидимые программы присутствуют в системе. её сотрудники сообщили, что все, кто критиковал ПО CyberPatrol, заблокированы по всем категориям.

Владелец компании CyberPatrol подал в суд на авторов этой программы, утверждая, что лицензия CyberPatrol запрещает инженерный анализ ПО компании. Он получил предварительное судебное заключение, запрещающее распространение ПО, но авторы программы cphack продали её владельцу компании за 1 долл. И согласились выполнить это постановление. Похоже, что авторы отступили. Владелец компании пытается доказать свои права на программу, выпущенную как общедоступное ПО (т.е. с лицензией GNU Public License).

2. Правила, регламенты и стратегия администрирования в ИС

2.3. Особенности реализации технологий администрирования в ИС

Многие компании оплачивают меньшее количество копий программных пакетов, чем на самом деле используют. Если об этом становится известно, то компания теряет гораздо больше, чем сэкономила на приобретении недостающего числа лицензий. Другие компании получают демоверсию дорогого пакета и взламывают её (меняют дату на компьютере, определяют лицензионный ключ и т.д.), чтобы пакет продолжал работать по истечении демонстрационного срока. Как системный администратор должен реагировать на предложения нарушить лицензионное соглашение и установить нелицензионные копии продукта на дополнительные машины? Что ему делать, если он обнаружит, что на обслуживаемых им компьютерах работает пиратское ПО? Как быть с условно-бесплатными программами, за которые так никогда и не заплатили?

Это сложный вопрос. К сожалению, руководство не всегда поддерживает администратора, предлагающего либо удалить нелицензионные копии пакетов, либо оплатить их. А ведь часто именно системный администратор подписывает лицензионное соглашение, требующее удалить демонстрационные копии после определённой даты, тогда как решение их не удалять принимает руководитель. Необходимо помнить, что речь идёт о личной и профессиональной честности как администратора сети, так и руководителя организации.

2. Правила, регламенты и стратегия администрирования в ИС

2.3. Особенности реализации технологий администрирования в ИС

Безопаснее всего ситуация, когда организация, являясь подписчиком всех телеконференций, не подвергает цензуре их статьи и не сокращает иерархию телеконференций на основании их содержания. Другое дело, когда для сокращения появляются основания технического характера (например, нет места на диске). Если иерархию телеконференций нужно сократить, сделайте это ближе к вершине дерева. Легче оправдать отказ от всей категории alt, чем объяснить, зачем удалили alt.sex.fetish.feet и оставили alt.sex.bestiality. hamsters.

Этот подход распространяется и на другие отношения с внешним миром. С юридической точки зрения, чем больше администратор сети контролирует использование Интернета пользователями, тем большую ответственность он может понести за их действия и публикации. Если он к тому же знает о противоправной, подсудной деятельности, то закон обязывает расследовать её и доложить о результатах в соответствующие органы.

По этой причине некоторые компании ограничивают данные, которые они вносят в журналы доступа на своих Web-узлах, сокращают время хранения журналов и не все их данные записывают в архивы и резервные копии. Для реализации подобной политики существует даже специальное ПО (например, Squid web cache), определяющее уровень протоколирования доступа, что позволяет системным администраторам разрешать возникающие проблемы и при этом не нарушать конфиденциальности действий пользователей.

Системные администраторы должны знать правила, действующие во всех подразделениях организации, и обеспечивать их неукоснительное соблюдение. При этом нужно учитывать, что не имеющие законной силы и противоречивые правила – это ещё хуже, чем их отсутствие (как с практической, так и с юридической точек зрения).

3. Технология управления безопасностью информации и ресурсов в автоматизированной системе

Обеспечение безопасности АС есть процесс управления рисками, следовательно, система защиты –это система управления, реализующая технологию обеспечения безопасности (управления безопасностью). Любая технология предусматривает определённый набор операций и процессов взаимодействия их исполнителей, направленный на достижение конечного результата (цели).

При разработке технологии управления решают следующие вопросы:

- определяют категории сотрудников, входящих в систему безопасности АС организации, и их функции;
- регламентируют порядок взаимодействия подразделений;
- разрабатывают перечень регламентируемых процессов и действий;
- составляют организационно-распорядительные и нормативно-методические документы.

Под технологией обеспечения безопасности информации и ресурсов в АС понимается определённое распределение функций и регламентация порядка их исполнения, а также порядка взаимодействия подразделений и сотрудников (должностных лиц) организации по обеспечению комплексной защиты ресурсов АС в процессе её эксплуатации.

3. Технология управления безопасностью информации и ресурсов в автоматизированной системе

К технологии управления безопасностью предъявляют определённые требования:

- соответствие современному уровню развития информационных технологий;
- учёт особенностей построения и функционирования различных подсистем АС;
- точная и своевременная реализация политики безопасности организации;
- минимизация затрат на реализацию самой технологии обеспечения безопасности;
- наличие полной и непротиворечивой правовой базы по вопросам обеспечения безопасности ИТ;
- чёткое распределение функций и порядка взаимодействия подразделений и должностных лиц организации по вопросам обеспечения безопасности ИТ на всех этапах жизненного цикла подсистем АС;
- наличие подразделения защиты информации, наделённого необходимыми полномочиями, которое отвечает за формирование и реализацию единой политики безопасности ИТ организации и осуществляет контроль и координацию действий подразделений и сотрудников организации по вопросам обеспечения безопасности ИТ.

3. Технология управления безопасностью информации и ресурсов в автоматизированной системе

При реализации технологии управления безопасностью АС осуществляют следующие мероприятия

- назначение и подготовка сотрудников, ответственных за организацию, реализацию функций и осуществление конкретных практических мероприятий по обеспечению безопасности информации и процессов её обработки;
- строгий учёт всех подлежащих защите ресурсов системы (информации, её носителей и процессов обработки) с определением требований к организационно-техническим мерам и средствам защиты;
- разработка реально выполнимых и непротиворечивых организационно распорядительных документов по вопросам обеспечения безопасности информации;
- реорганизация технологических процессов обработки информации в АС с учётом требований по безопасности ИТ;
- поддержание необходимого уровня защищённости и целостности технических средств;
- регламентация процессов обработки подлежащей защите информации с применением средств автоматизации при участии сотрудников структурных подразделений, использующих АС, и персонала, осуществляющего обслуживание и модификацию программных и технических средств АС, в соответствии с организационно-распорядительными документами по вопросам обеспечения безопасности ИТ;

3. Технология управления безопасностью информации и ресурсов в автоматизированной системе

- контроль за соблюдением сотрудниками подразделений – пользователями и обслуживающим АС персоналом – требований по обеспечению безопасности информации;
- проведение постоянного анализа эффективности и достаточности принятых мер и средств защиты информации;
- разработка и реализация предложений по совершенствованию системы защиты информации в АС.

3. Технология управления безопасностью информации и ресурсов в автоматизированной системе

3.1. Институт ответственных за обеспечение информационной безопасности

Обеспечение информационной безопасности – это непрерывный процесс, основное содержание которого составляет управление рисками через управление людьми, ресурсами, средствами защиты и т. п.

Обслуживающий персонал и конечные пользователи АС – неотъемлемая часть АС и от того, каким образом они реализуют свои функции в системе, существенно зависит не только её функциональность (эффективность решения задач), но и безопасность.

Уровень информационной безопасности организации существенно зависит от деятельности следующих категорий сотрудников и должностных лиц организации:

- руководителей организации, определяющих цели и задачи функционирования АС;
- сотрудников подразделения защиты информации, оценивающих состояние безопасности АС, определяющих требования к системе защиты, разрабатывающих организационно-распорядительные документы, внедряющих и администрирующих специализированные дополнительные средства защиты (администраторов безопасности);
- системных администраторов штатных средств защиты (ОС, СУБД и т. п.);
- сотрудников подразделения эксплуатации технических средств (ТС),

3. Технология управления безопасностью информации и ресурсов в автоматизированной системе

3.1. Институт ответственных за обеспечение информационной безопасности

- сотрудников подразделения внедрения и сопровождения ПО, обеспечивающих нормальное функционирование и установленный порядок инсталляции и модификации прикладных программ;
- программистов, осуществляющих разработку (приобретение и адаптацию) необходимых прикладных программ для автоматизации деятельности сотрудников организации;
- сотрудников структурных подразделений конечных пользователей – АС, решающих свои функциональные задачи с применением средств автоматизации.

Кроме того, на безопасность ИТ организации могут оказывать влияние посторонние лица и сторонние организации, предпринимающие попытки вмешательства в процесс нормального функционирования АС или несанкционированного доступа к информации как локально, так и удалённо.

3. Технология управления безопасностью информации и ресурсов в автоматизированной системе

3.2. Влияние на безопасность информационных технологий руководства организации.

Руководство принимает стратегические решения по вопросам обеспечения безопасности ИТ и утверждает основные документы, регламентирующие порядок функционирования и развития АС, обеспечивающий безопасную обработку и использование защищаемой информации.

Руководство определяет критичность процессов, ресурсов и степень их защиты, а также координирует деятельность по управлению и распределению обязанностей по обеспечению безопасности ИТ между службами безопасности и автоматизации.

В соответствии со стандартом ISO 27002 руководство должно показывать свою заинтересованность в вопросах безопасности ИТ, оказывать поддержку в распространении политики безопасности ИТ среди сотрудников организации и проводить регулярные совещания по вопросам корректировки политики безопасности, ИТ, и координации действий персонала.

3. Технология управления безопасностью информации и ресурсов в автоматизированной системе

3.2. Влияние на безопасность информационных технологий руководства организации.

Для того чтобы добиться понимания и осознания важности проблем безопасности ИТ, руководителями используются различные меры, например, такие:

- извлечение максимальной пользы из любых инцидентов с акцентом на важность решений вопросов по обеспечению безопасности ИТ;
- организация показательных мероприятий слабости парольной защиты – (например, демонстрация проведение подобных мероприятий требует предварительного согласования с руководством, документального оформления и осторожности при реализации;
- демонстрация документов других организаций по вопросам обеспечения безопасности ИТ.

3. Технология управления безопасностью информации и ресурсов в автоматизированной системе

3.3. Влияние на безопасность информационных технологий службы безопасности.

Наиболее важным звеном, оказывающим влияние на безопасность ИТ организации, являются аналитики и администраторы средств защиты, контроля и управления безопасностью – аналитики отвечают за анализ состояния безопасности ИТ, определение требований к защищённости различных подсистем АС, выбор методов и средств защиты; администраторы средств защиты, контроля и управления безопасностью отвечают за эффективное применение специализированных средств защиты.

Влияние на безопасность информационных технологий подразделения автоматизации. Наиболее существенное влияние на безопасность ИТ организации в подразделении автоматизации оказывают специалисты служб разработки, внедрения и сопровождения ПО, эксплуатации технических средств и общего программного обеспечения, системные администраторы.

Влияние программистов может быть как непреднамеренным (ошибки), так и преднамеренным (закладки, люки). Практика показывает, что ошибки кода присутствуют практически в каждой программе.

3. Технология управления безопасностью информации и ресурсов в автоматизированной системе

3.3. Влияние на безопасность информационных технологий службы безопасности.

Администраторы серверов, приложений и баз данных отвечают за эффективное применение штатных средств защиты и разграничение доступа всех используемых ОС и СУБД.

Для обеспечения безопасности ИТ необходимо повышение ответственности на основе регламентации процессов разработки, отладки и внедрения ПО, т. е. разделение сотрудников на группы разрабатывающих, тестирующих, внедряющих и сопровождающих ПО.

Влияние на безопасность информационных технологий сотрудников структурных подразделений организации. Совершение ошибок сотрудниками структурных подразделений (конечными пользователями системы) способствует порождению угроз, которые затем могут быть использованы злоумышленниками для нанесения вреда организации и её сотрудникам.

К числу таких угроз можно отнести:

- создание предпосылок к осуществлению НСД со стороны других лиц (уязвимостей, каналов проникновения) к критичным ресурсам системы;
- разглашение конфиденциальной информации (сведений, составляющих коммерческую тайну организации, персональных данных, паролей и др.);

3. Технология управления безопасностью информации и ресурсов в автоматизированной системе

3.3. Влияние на безопасность информационных технологий службы безопасности.

- заражение рабочих станций вирусами, троянскими и другими вредоносными программами (внедрение шпионских кодов);
- создание помех для основных производственных процессов или остановка их работы

Злоумышленники преследуют определённые цели:

- порча или утрата материального имущества (технических средств);
- искажение или утрата файлов с важной информацией;
- потеря конкурентных преимуществ в результате разглашения сведений, составляющих коммерческую тайну;
- дезорганизация или снижение эффективности производственных процессов (нарушение работоспособности подсистем);
- непроизводительные траты ресурсов (материальных, информационных, операционных, рабочего времени и др.);
- судебные иски к организации, её руководителям и сотрудникам со стороны государственных органов, других юридических и физических лиц;
- потеря деловой репутации организации (с последующей потерей клиентов, партнёров и т. п.);
- нанесение физического или морального ущерба сотрудникам организации или третьим лицам.

3. Технология управления безопасностью информации и ресурсов в автоматизированной системе

3.3. Влияние на безопасность информационных технологий службы безопасности.

Смысл безопасности ИТ состоит в жёсткой регламентации деятельности сотрудников, сочетающейся с высокой исполнительской дисциплиной.

Необходимо учитывать, что регламентация деятельности сотрудников, непосредственно не подчинённых службе безопасности, может привести к возникновению конфликтных ситуаций, поэтому дополнительные функции сотрудников должны быть чётко определены в соответствующих инструкциях.

4. Программы безопасности верхнего и процедурного уровня

4.1. Административный уровень информационной безопасности

Выделяют два уровня программ информационной безопасности – административный (верхний) и процедурный (служебный).

К административному уровню информационной безопасности относятся действия общего характера, предпринимаемые руководством организации.

Главная цель мер административного уровня – сформировать программу работ в области информационной безопасности и обеспечить её выполнение, выделяя необходимые ресурсы и контролируя состояние дел.

Основой программы является политика безопасности, отражающая подход организации к защите своих информационных активов. Руководство каждой организации должно осознать необходимость поддержания режима безопасности и выделения на эти цели значительных ресурсов.

Политика безопасности строится на основе анализа рисков, которые признаются реальными для информационной системы организации. Когда риски проанализированы и стратегия защиты определена, составляется программа обеспечения информационной безопасности. Под эту программу выделяются ресурсы, назначаются ответственные, определяется порядок контроля выполнения программы и т.п.

4. Программы безопасности верхнего и процедурного уровня

4.1. Административный уровень информационной безопасности

Термин «политика безопасности» является не совсем точным переводом английского словосочетания «security policy», однако в данном случае калька лучше отражает смысл этого понятия, чем лингвистически более верные «правила безопасности». Мы будем иметь в виду не отдельные правила или их наборы (такого рода решения выносятся на процедурный уровень, речь о котором впереди), а стратегию организации в области информационной безопасности.

Для выработки стратегии и проведения её в жизнь нужны, несомненно, политические решения, принимаемые на самом высоком уровне.

Под политикой безопасности мы будем понимать совокупность документированных решений, принимаемых руководством организаций, направленных на защиту информации и ассоциированных с ней ресурсов.

Такая трактовка, конечно, гораздо шире, чем набор правил разграничения доступа (именно это означал термин «security policy» в «Оранжевой книге» и в построенных на её основе нормативных документах других стран).

ИС организации и связанные с ней интересы субъектов – это сложная система, для рассмотрения которой необходимо применять объектно-ориентированный подход и понятие уровня детализации.

4. Программы безопасности верхнего и процедурного уровня

4.1. Административный уровень информационной безопасности

Целесообразно выделить, по крайней мере, три таких уровня, что сделаем далее.

Чтобы рассматривать ИС предметно, с использованием актуальных данных, следует составить карту информационной системы.

Эта карта, разумеется, должна быть изготовлена в объектно-ориентированном стиле, с возможностью варьировать не только уровень детализации, но и видимые грани объектов. Техническим средством составления, сопровождения и визуализации подобных карт может служить свободно распространяемый каркас какой-либо системы управления.

4. Программы безопасности верхнего и процедурного уровня

4.2. Политика безопасности организации

Политика безопасности организации в области ИТ – это совокупность документируемых решений в виде программных, аппаратных, организационных, административных, юридических, физических мер, методов, средств, правил и инструкций, регламентирующих все аспекты деятельности организации в области безопасности ИТ.

Основная цель политики безопасности – информирование пользователей, сотрудников и руководства о наложенных на них обязательных требованиях по защите технологии и информационных ресурсов.

Все документально оформленные решения, формирующие политику безопасности ИТ, утверждаются руководством и предоставляются сотрудникам организации для ознакомления.

При определении политики безопасности должны соблюдаться следующие условия:

- непрерывность работы и восстановление АС;
- конфиденциальность стандартных сервисов (электронная почта, Интернет, виртуальные частные сети (VPN), мобильные пользователи);

4. Программы безопасности верхнего и процедурного уровня

4.2. Политика безопасности организации

- аутентификация (пароли, рекомендации по аутентификации удалённых субъектов и использованию аутентифицирующих устройств);
- разграничение доступа и привилегии для различных категорий сотрудников (пользователей, системных администраторов, администраторов безопасности, руководителей);
- блокирование вирусов и других вредоносных программ;
- обучение персонала по вопросам безопасности ИТ;
- защита от недекларированных возможностей ПО;
- ликвидация последствий нарушения политики безопасности и ответственность нарушителей;
- аудит и обновление политики безопасности.

К сожалению, на практике после внедрения в организациях систем обеспечения безопасности возможны следующие типичные проблемы:

- отсутствие необходимой организационной основы для согласованных действий подразделений организации по выработке и реализации единой политики безопасности ИТ;
- неполнота, противоречивость и несоответствие требованиям законодательства РФ нормативно-правовой базы организации по вопросам обеспечения безопасности ИТ.

4. Программы безопасности верхнего и процедурного уровня

4.2. Политика безопасности организации

Для оценки текущего состояния ИТ в организации существуют различные методики и модели зрелости или оптимизации ИТ-инфраструктуры, предлагаемые известными исследовательскими и консалтинговыми организациями в области ИТ (например, Infrastructure Maturity Model, Gartner Group, Architecture Maturity Model, MTI, Infrastructure Optimization Model, Microsoft). Набор сервисов в моделях зрелости называют уровнем зрелости. Так,в Infrastructure Maturity Model (Gartner Group) определены четыре уровня зрелости (в сфере обеспечения ИБ):

0-й уровень: информационной безопасностью в компании никто не занимается, руководство компании не осознает важности проблем информационной безопасности; финансирование отсутствует; информационная безопасность реализуется штатными средствами операционных систем, СУБД и приложений (парольная защита, разграничение доступа к ресурсам и сервисам);

1-й уровень: информационная безопасность рассматривается руководством как чисто «техническая» проблема, отсутствует единая концепция развития системы обеспечения информационной безопасности компании; финансирование осуществляется в рамках общего ИТ-бюджета; информационная безопасность реализуется средствами нулевого уровня, а также средствами резервного копирования, антивирусными средствами, межсетевыми экранами, средствами организации VPN (построения виртуальных частных сетей), т.е. используются традиционные средства защиты

4. Программы безопасности верхнего и процедурного уровня

4.2. Политика безопасности организации

2-й уровень: информационная безопасность рассматривается руководством как комплекс организационных и технических мероприятий; существует понимание важности информационной безопасности для производственных процессов; имеется программа развития системы обеспечения информационной безопасности компании; финансирование осуществляется по отдельной строке бюджета; дополнительно к средствам первого уровня применяют средства усиленной аутентификации, анализа почтовых сообщений и веб-контента, обнаружения вторжений (IDS), анализа защищённости, однократной аутентификации (SSO), инфраструктуру открытых ключей (PKI) и организационные меры (внутренний и внешний аудит, анализ рисков, политика информационной безопасности, положения, процедуры, регламенты и руководства);

3-й уровень: информационная безопасность – часть корпоративной культуры, выделена штатная единица – старший администратор по вопросам обеспечения информационной безопасности (CISA); финансирование ведётся в рамках отдельного бюджета, а в дополнение к средствам второго уровня реализована система управления информационной безопасностью; сформирована группа реагирования на инциденты нарушения информационной безопасности (CSIRT); подписано соглашение об уровне сервиса (SLA).

4. Программы безопасности верхнего и процедурного уровня

4.2. Политика безопасности организации

С практической точки зрения политику безопасности целесообразно рассматривать на трёх уровнях детализации. К верхнему уровню можно отнести решения, затрагивающие организацию в целом. Они носят весьма общий характер и, как правило, исходят от руководства организации. Примерный список подобных решений может включать в себя следующие элементы:

- решение сформировать или пересмотреть комплексную программу обеспечения информационной безопасности, назначение ответственных за продвижение программы;
- формулировку целей, которые преследует организация в области информационной безопасности, определение общих направлений в достижении этих целей;
- обеспечение базы для соблюдения законов и правил;
- формулировку административных решений по тем вопросам реализации программы безопасности, которые должны рассматриваться на уровне организации в целом.

4. Программы безопасности верхнего и процедурного уровня

4.2. Политика безопасности организации

Для политики верхнего уровня цели организации в области информационной безопасности формулируются в терминах целостности, доступности и конфиденциальности. Если организация отвечает за поддержание критически важных баз данных, на первом плане может стоять уменьшение числа потерь, повреждений или искажений данных. Для организации, занимающейся продажей компьютерной техники, вероятно, важна актуальность информации о предоставляемых услугах и ценах и её доступность максимальному числу потенциальных покупателей. Руководство режимного предприятия, в первую очередь, заботится о защите от несанкционированного доступа, то есть о конфиденциальности.

На верхний уровень выносится управление защитными ресурсами и координация использования этих ресурсов, выделение специального персонала для защиты критически важных систем и взаимодействие с другими организациями, обеспечивающими или контролирующими режим безопасности.

Политика верхнего уровня должна чётко очерчивать сферу своего влияния. Возможно, это будут все компьютерные системы организации (или даже больше, если политика регламентирует некоторые аспекты использования сотрудниками своих домашних компьютеров). Возможна, однако, и такая ситуация, когда в сферу влияния включаются лишь наиболее важные системы.

4. Программы безопасности верхнего и процедурного уровня

4.2. Политика безопасности организации

В политике должны быть определены обязанности должностных лиц по выработке программы безопасности и проведению её в жизнь. В этом смысле политика безопасности является основой подотчётности персонала.

Политика верхнего уровня имеет дело с тремя аспектами законопослушности и исполнительской дисциплины.

Во-первых, организация должна соблюдать существующие законы.

Во-вторых, следует контролировать действия лиц, ответственных за выработку программы безопасности.

Наконец, необходимо обеспечить определённую степень исполнительности персонала, а для этого нужно выработать систему поощрений и наказаний.

Вообще говоря, на верхний уровень следует выносить минимум вопросов. Подобное вынесение целесообразно, когда оно сулит значительную экономию средств или когда иначе поступить просто невозможно.

4. Программы безопасности верхнего и процедурного уровня

4.2. Политика безопасности организации

Британский стандарт BS 7799:1995 рекомендует включать в документ, характеризующий политику безопасности организации, следующие разделы:

- вводный, подтверждающий озабоченность высшего руководства проблемами ИБ;
- организационный, содержащий описание подразделений, комиссий, групп и т. д., отвечающих за работы в области информационной безопасности;
- классификационный, описывающий имеющиеся в организации материальные и информационные ресурсы и необходимый уровень их защиты;
- штатный, характеризующий меры безопасности, применяемые к персоналу (описание должностей с точки зрения информационной безопасности, организация обучения и переподготовки персонала, порядок реагирования на нарушения режима безопасности и т.п.);
- раздел, освещающий вопросы физической защиты;
- управляющий раздел, описывающий подход к управлению компьютерами и компьютерными сетями;
- раздел, описывающий правила разграничения доступа к производственной информации;
- раздел, характеризующий порядок разработки и сопровождения систем;
- раздел, описывающий меры, направленные на обеспечение непрерывной работы организации;
- юридический раздел, подтверждающий соответствие политики безопасности

4. Программы безопасности верхнего и процедурного уровня

4.2. Политика безопасности организации

К среднему уровню можно отнести вопросы, касающиеся отдельных аспектов информационной безопасности, но важные для различных эксплуатируемых организацией систем. Примеры таких вопросов – отношение к передовым (но, возможно, недостаточно проверенным) технологиям, доступ в Internet (как совместить свободу доступа к информации с защитой от внешних угроз?), использование домашних компьютеров, применение пользователями неофициального программного обеспечения и т.д.

Политика среднего уровня должна для каждого аспекта освещать следующие темы:

- Описание аспекта
- Область применения
- Позиция организации по данному аспекту
- Роли и обязанности
- Законопослушность
- Точки контакта

Описание аспекта. Например, если рассмотреть применение пользователями неофициального программного обеспечения, последнее можно определить как ПО, которое не было одобрено и/или закуплено на уровне организации.

4. Программы безопасности верхнего и процедурного уровня

4.2. Политика безопасности организации

Область применения. Следует определить, где, когда, как, по отношению к кому и чему применяется данная политика безопасности. Например, касается ли политика, связанная с использованием неофициального программного обеспечения, организаций-субподрядчиков? Затрагивает ли она сотрудников, пользующихся портативными и домашними компьютерами и вынужденных переносить информацию на производственные машины?

Позиция организации по данному аспекту. Продолжая пример с неофициальным программным обеспечением, можно представить себе позиции полного запрета, выработки процедуры приёмки подобного ПО и т.п. Позиция может быть сформулирована и в гораздо более общем виде как набор целей, которые преследует организация в данном аспекте. Вообще стиль документов, определяющих политику безопасности (как и их перечень), в разных организациях может сильно отличаться.

Роли и обязанности. В «политический» документ необходимо включить информацию о должностных лицах, ответственных за реализацию политики безопасности. Например, если для использования неофициального программного обеспечения сотрудникам требуется разрешение руководства, должно быть известно, у кого и как его можно получить. Если неофициальное программное обеспечение использовать нельзя, следует знать, кто следит за выполнением данного правила.

4. Программы безопасности верхнего и процедурного уровня

4.2. Политика безопасности организации

Законопослушность. Политика должна содержать общее описание запрещённых действий и наказаний за них.

Точки контакта. Должно быть известно, куда следует обращаться за разъяснениями, помощью и дополнительной информацией. Обычно «точкой контакта» служит определённое должностное лицо, а не конкретный человек, занимающий в данный момент данный пост.

Политика безопасности нижнего уровня относится к конкретным информационным сервисам. Она включает в себя два аспекта — цели и правила их достижения, поэтому её порой трудно отделить от вопросов реализации. В отличие от двух верхних уровней рассматриваемая политика должна быть определена более подробно. Есть много вещей, специфичных для отдельных видов услуг, которые нельзя единым образом регламентировать в рамках всей организации. В то же время эти вещи настолько важны для обеспечения режима безопасности, что относящиеся к ним решения должны приниматься на управленческом, а не техническом уровне. Приведём несколько примеров вопросов, на которые следует дать ответ в политике безопасности нижнего уровня:

- кто имеет право доступа к объектам, поддерживаемым сервисом?
- при каких условиях можно читать и модифицировать данные?
- как организован удалённый доступ к сервису?

4. Программы безопасности верхнего и процедурного уровня

4.2. Политика безопасности организации

При формулировке целей политики нижнего уровня можно исходить из соображений целостности, доступности и конфиденциальности, но нельзя на этом останавливаться. её цели должны быть более конкретными. Например, если речь идёт о системе расчёта заработной платы, можно поставить цель, чтобы только сотрудникам отдела кадров и бухгалтерии позволялось вводить и модифицировать информацию. В более общем случае цели должны связывать между собой объекты сервиса и действия с ними.

Из целей выводятся правила безопасности, описывающие, кто, что и при каких условиях может делать. Чем подробнее правила, чем более формально они изложены, тем проще поддержать их выполнение программно-техническими средствами. С другой стороны, слишком жёсткие правила могут мешать работе пользователей, вероятно, их придётся часто пересматривать. Руководству предстоит найти разумный компромисс, когда за приемлемую цену будет обеспечен приемлемый уровень безопасности, а сотрудники не окажутся чрезмерно связаны. Обычно наиболее формально задаются права доступа к объектам ввиду особой важности данного вопроса.

4. Программы безопасности верхнего и процедурного уровня

4.3. Программа безопасности

После того как сформулирована политика безопасности, можно приступать к составлению программы её реализации и собственно к реализации.

Чтобы понять и реализовать какую-либо программу, её нужно структурировать по уровням, обычно в соответствии со структурой организации. В простейшем и самом распространённом случае достаточно двух уровней – верхнего, или центрального, который охватывает всю организацию, и нижнего, или служебного, который относится к отдельным услугам или группам однородных сервисов.

Программу верхнего уровня возглавляет лицо, отвечающее за информационную безопасность организации. У этой программы следующие главные цели:

- управление рисками (оценка рисков, выбор эффективных средств защиты);
- координация деятельности в области информационной безопасности, пополнение и распределение ресурсов;
- стратегическое планирование;
- контроль деятельности в области информационной безопасности.

В рамках программы верхнего уровня принимаются стратегические решения по обеспечению безопасности, оцениваются технологические новинки. Информационные технологии развиваются очень быстро, и необходимо иметь чёткую политику отслеживания и внедрения новых средств.

4. Программы безопасности верхнего и процедурного уровня

4.3. Программа безопасности

Контроль деятельности в области безопасности имеет двустороннюю направленность. Во-первых, необходимо гарантировать, что действия организации не противоречат законам. При этом следует поддерживать контакты с внешними контролирующими организациями. Во-вторых, нужно постоянно отслеживать состояние безопасности внутри организации, реагировать на случаи нарушений и дорабатывать защитные меры с учётом изменения обстановки.

Следует подчеркнуть, что программа верхнего уровня должна занимать строго определённое место в деятельности организации, она должна официально приниматься и поддерживаться руководством, а также иметь определённый штат и бюджет.

Цель программы нижнего уровня – обеспечить надёжную и экономичную защиту конкретного сервиса или группы однородных сервисов. На этом уровне решается, какие следует использовать механизмы защиты; закупаются и устанавливаются технические средства; выполняется повседневное администрирование; отслеживается состояние слабых мест и т.п. Обычно за программу нижнего уровня отвечают администраторы сервисов.

4. Программы безопасности верхнего и процедурного уровня

4.3. Программа безопасности

Синхронизация программы безопасности с жизненным циклом систем

Если синхронизировать программу безопасности нижнего уровня с жизненным циклом защищаемого сервиса, можно добиться большего эффекта с меньшими затратами. Программисты знают, что добавить новую возможность к уже готовой системе на порядок сложнее, чем изначально спроектировать и реализовать её. То же справедливо и для информационной безопасности.

В жизненном цикле информационного сервиса можно выделить следующие этапы:

- инициация – выявляется необходимость в приобретении нового сервиса, документируется его предполагаемое назначение;
- закупка – на данном этапе составляются спецификации, прорабатываются варианты приобретения, выполняется собственно закупка;
- установка – сервис устанавливается, конфигурируется, тестируется и вводится в эксплуатацию;
- эксплуатация –сервис не только работает и администрируется, но и подвергается модификациям;
- выведение из эксплуатации – происходит переход на новый сервис.

Рассмотрим действия, выполняемые на каждом из этапов, более подробно.

4. Программы безопасности верхнего и процедурного уровня

4.3. Программа безопасности

На этапе инициации оформляется понимание того, что необходимо приобрести новый или значительно модернизировать существующий сервис; определяется, какими характеристиками и какой функциональностью он должен обладать; оцениваются финансовые и иные ограничения.

С точки зрения безопасности важнейшим действием здесь является оценка критичности как самого сервиса, так и информации, которая с его помощью будет обрабатываться. Требуется сформулировать ответы на следующие вопросы:

- какого рода информация предназначается для обслуживания новым сервисом?
- каковы возможные последствия нарушения конфиденциальности, целостности и доступности этой информации?
- каковы угрозы, по отношению к которым сервис и информация будут наиболее уязвимы?
- есть ли какие-либо особенности нового сервиса (например, территориальная распределённость компонентов), требующие принятия специальных процедурных мер?
- каковы характеристики персонала, имеющие отношение к безопасности (квалификация, благонадёжность)?
- каковы законодательные положения и внутренние правила, которым должен соответствовать новый сервис?

4. Программы безопасности верхнего и процедурного уровня

4.3. Программа безопасности

Результаты оценки критичности являются отправной точкой в составлении спецификаций. Кроме того, они определяют ту меру внимания, которую служба безопасности организации должна уделять новому сервису на последующих этапах его жизненного цикла.

Этап закупки – один из самых сложных. Нужно окончательно сформулировать требования к защитным средствам нового сервиса, к компании, которая может претендовать на роль поставщика, и к квалификации, которой должен обладать персонал, использующий или обслуживающий закупаемый продукт.

Все эти сведения оформляются в виде спецификации, куда входят не только аппаратура и программы, но и документация, обслуживание, обучение персонала. Разумеется, особое внимание должно уделяться вопросам совместимости нового сервиса с существующей конфигурацией.

Подчеркнём также, что нередко средства безопасности являются необязательными компонентами коммерческих продуктов, и нужно проследить, чтобы соответствующие пункты не выпали из спецификации.

4. Программы безопасности верхнего и процедурного уровня

4.3. Программа безопасности

Когда продукт закуплен, его необходимо установить. Несмотря на кажущуюся простоту, установка является очень ответственным делом.

Во-первых, новый продукт следует сконфигурировать. Как правило, коммерческие продукты поставляются с отключёнными средствами безопасности; их необходимо включить и должным образом настроить. Для большой организации, где много пользователей и данных, начальная настройка может стать весьма трудоёмким и ответственным делом.

Во-вторых, новый сервис нуждается в процедурных регуляторах. Следует позаботиться о чистоте и охране помещения, о документах, регламентирующих использование сервиса, о подготовке планов на случай экстренных ситуаций, об организации обучения пользователей и т.п.

После принятия перечисленных мер необходимо провести тестирование. Его полнота и комплексность могут служить гарантией безопасности эксплуатации в штатном режиме.

4. Программы безопасности верхнего и процедурного уровня

4.3. Программа безопасности

Период эксплуатации – самый длительный и сложный. С психологической точки зрения наибольшую опасность в это время представляют незначительные изменения в конфигурации сервиса, в поведении пользователей и администраторов. Если безопасность не поддерживать, она ослабевает. Пользователи не столь ревностно выполняют должностные инструкции, администраторы менее тщательно анализируют регистрационную информацию. То один, то другой пользователь получает дополнительные привилегии. Кажется, что в сущности ничего не изменилось; на самом же деле от былой безопасности не осталось и следа.

Для борьбы с эффектом медленных изменений приходится прибегать к периодическим проверкам безопасности сервиса. Разумеется, после значительных модификаций подобные проверки являются обязательными.

При выведении из эксплуатации затрагиваются аппаратно-программные компоненты сервиса и обрабатываемые им данные. Аппаратура продаётся, утилизируется или выбрасывается. Только в специфических случаях необходимо заботиться о физическом разрушении аппаратных компонентов, хранящих конфиденциальную информацию. Программы, вероятно, просто стираются, если иное не предусмотрено лицензионным соглашением.

4. Программы безопасности верхнего и процедурного уровня

4.3. Программа безопасности

При выведении данных из эксплуатации их обычно переносят на другую систему, архивируют, выбрасывают или уничтожают. Если архивирование производится с намерением впоследствии прочитать данные в другом месте, следует позаботиться об аппаратно-программной совместимости средств чтения и записи.

Информационные технологии развиваются очень быстро, и через несколько лет устройств, способных прочитать старый носитель, может просто не оказаться. Если данные архивируются в зашифрованном виде, необходимо сохранить ключ и средства расшифровки.

При архивировании и хранении архивной информации нельзя забывать о поддержании конфиденциальности данных.

4. Программы безопасности верхнего и процедурного уровня

4.4. Управление рисками

Управление рисками рассматривается на административном уровне ИБ, поскольку только руководство организации способно выделить необходимые ресурсы, инициировать и контролировать выполнение соответствующих программ.

Управление рисками, равно как и выработка собственной политики безопасности, актуально только для тех организаций, информационные системы и/или обрабатываемые данные которых можно считать нестандартными. Обычную организацию вполне устроит типовой набор защитных мер, выбранный на основе представления о типичных рисках или вообще без всякого анализа рисков (особенно это верно с формальной точки зрения, в свете проанализированного нами ранее российского законодательства в области ИБ). Можно провести аналогию между индивидуальным строительством и получением квартиры в районе массовой застройки. В первом случае необходимо принять множество решений, оформить большое количество бумаг, во втором достаточно – определиться лишь с несколькими параметрами.

Использование информационных систем связано с определённой совокупностью рисков. Когда возможный ущерб неприемлемо велик, необходимо принять экономически оправданные меры защиты. Периодическая (пере)оценка рисков необходима для контроля эффективности деятельности в области безопасности и для учёта изменений обстановки.

4. Программы безопасности верхнего и процедурного уровня

4.4. Управление рисками

С количественной точки зрения уровень риска является функцией вероятности реализации определённой угрозы (использующей некоторые уязвимые места), а также величины возможного ущерба.

Таким образом, суть мероприятий по управлению рисками состоит в том, чтобы оценить их размер, выработать эффективные и экономичные меры снижения рисков, а затем убедиться, что риски заключены в приемлемые рамки (и остаются таковыми). Следовательно, управление рисками включает в себя два вида деятельности, которые чередуются циклически:

- (пере)оценка (измерение) рисков;
- выбор эффективных и экономичных защитных средств (нейтрализация рисков).

По отношению к выявленным рискам возможны следующие действия:

- ликвидация риска (например, за счёт устранения причины);
- уменьшение риска (например, за счёт использования дополнительных защитных средств);
- принятие риска (и выработка плана действия в соответствующих условиях);
- переадресация риска (например, путём заключения страхового соглашения).

4. Программы безопасности верхнего и процедурного уровня

4.4. Управление рисками

Процесс управления рисками можно разделить на следующие этапы:

1. Выбор анализируемых объектов и уровня детализации их рассмотрения.
2. Выбор методологии оценки рисков.
3. Идентификация активов.
4. Анализ угроз и их последствий, выявление уязвимых мест в защите.
5. Оценка рисков.
6. Выбор защитных мер.
7. Реализация и проверка выбранных мер.
8. Оценка остаточного риска.

Этапы 6 и 7 относятся к выбору защитных средств (нейтрализации рисков), остальные – к оценке рисков.

Уже перечисление этапов показывает, что управление рисками – процесс циклический. По существу, последний этап – это оператор конца цикла, предписывающий вернуться к началу. Риски нужно контролировать постоянно, периодически проводя их переоценку. Отметим, что добросовестно выполненная и тщательно документированная первая оценка может существенно упростить последующую деятельность.

4. Программы безопасности верхнего и процедурного уровня

4.4. Управление рисками

Управление рисками, как и любую другую деятельность в области информационной безопасности, необходимо интегрировать в жизненный цикл ИС. Тогда эффект оказывается наибольшим, а затраты – минимальными. Ранее мы определили пять этапов жизненного цикла. Кратко опишем, что может дать управление рисками на каждом из них.

На этапе инициации известные риски следует учесть при выработке требований к системе вообще и средствам безопасности в частности.

На этапе закупки (разработки) знание рисков поможет выбрать соответствующие архитектурные решения, которые играют ключевую роль в обеспечении безопасности.
На этапе установки выявленные риски следует учитывать при конфигурировании, тестировании и проверке ранее сформулированных требований, а полный цикл управления рисками должен предшествовать внедрению системы в эксплуатацию.

На этапе эксплуатации управление рисками должно сопровождать все существенные изменения в системе.

При выведении системы из эксплуатации управление рисками помогает

4. Программы безопасности верхнего и процедурного уровня

4.5. Подготовительные этапы управления рисками

Опишем первые три этапа процесса управления рисками. Выбор анализируемых объектов и уровня детализации их рассмотрения – первый шаг в оценке рисков. Для небольшой организации допустимо рассматривать всю информационную инфраструктуру, однако если организация крупная, всеобъемлющая оценка может потребовать неприемлемых затрат времени и сил.

В таком случае следует сосредоточиться на наиболее важных сервисах, заранее соглашаясь с приближённостью итоговой оценки.

Если важных сервисов все ещё много, выбираются те из них, риски для которых заведомо велики или неизвестны.

Мы уже указывали на целесообразность создания карты информационной системы организации. Для управления рисками подобная карта особенно важна, поскольку она наглядно показывает, какие сервисы выбраны для анализа, а какими пришлось пренебречь. Если ИС меняется, а карта поддерживается в актуальном состоянии, то при переоценке рисков сразу станет ясно, какие новые или существенно изменившиеся сервисы нуждаются в рассмотрении.

4. Программы безопасности верхнего и процедурного уровня

4.5. Подготовительные этапы управления рисками

Вообще говоря, уязвимым является каждый компонент информационной системы – от сетевого кабеля, который могут прогрызть мыши, до базы данных, которая может быть разрушена из-за неумелых действий администратора.

Как правило, в сферу анализа невозможно включить каждый винтик и каждый байт. Приходится останавливаться на некотором уровне детализации, опять-таки отдавая себе отчёт в приближённости оценки.

Для новых систем предпочтителен детальный анализ; старая система, подвергшаяся небольшим модификациям, может быть проанализирована более поверхностно.

Очень важно выбрать разумную методологию оценки рисков. Целью оценки является получение ответа на два вопроса: приемлемы ли существующие риски и если нет, то какие защитные средства стоит использовать. Значит, оценка должна быть количественной, допускающей сопоставление с заранее выбранными границами допустимости и расходами на реализацию новых регуляторов безопасности.

Управление рисками – типичная оптимизационная задача, и существует довольно много программных продуктов, способных помочь в её решении (иногда подобные продукты просто прилагаются к книгам по информационной

4. Программы безопасности верхнего и процедурного уровня

4.5. Подготовительные этапы управления рисками

Принципиальная трудность, однако, состоит в неточности исходных данных. Можно, конечно, попытаться получить для всех анализируемых величин денежное выражение, высчитать все с точностью до копейки, но большого смысла в этом нет. Практичнее пользоваться условными единицами. В простейшем и вполне допустимом случае можно пользоваться трёхбалльной шкалой. Далее мы продемонстрируем, как это делается.

При идентификации активов, то есть тех ресурсов и ценностей, которые организация пытается защитить, следует, конечно, учитывать не только компоненты информационной системы, но и поддерживающую инфраструктуру, персонал, а также нематериальные ценности, такие как репутация организации. Отправной точкой здесь является представление о миссии организации, то есть об основных направлениях деятельности, которые желательно (или необходимо) сохранить в любом случае. Выражаясь объектно-ориентированным языком, следует, в первую очередь, описать внешний интерфейс организации, рассматриваемой как абстрактный объект.

Одним из главных результатов процесса идентификации активов является получение детальной информационной структуры организации и способов её (структуры) использования. Эти сведения целесообразно нанести на карту ИС в качестве граней соответствующих объектов.

4. Программы безопасности верхнего и процедурного уровня

4.5. Подготовительные этапы управления рисками

Информационной основой сколько-нибудь крупной организации является сеть, поэтому в число аппаратных активов следует включить компьютеры (серверы, рабочие станции, ПК), периферийные устройства, внешние интерфейсы, кабельное хозяйство, активное сетевое оборудование (мосты, маршрутизаторы и т.п.). К программным активам, вероятно, будут отнесены операционные системы (сетевая, серверные и клиентские), прикладное программное обеспечение, инструментальные средства, средства управления сетью и отдельными системами. Важно зафиксировать, где (в каких узлах сети) хранится программное обеспечение и из каких узлов оно используется. Третьим видом информационных активов являются данные, которые хранятся, обрабатываются и передаются по сети. Следует классифицировать данные по типам и степени конфиденциальности, выявить места их хранения и обработки, способы доступа к ним. Все это важно для оценки последствий нарушений информационной безопасности.

Управление рисками – процесс далеко не линейный. Практически все его этапы связаны между собой, и по завершении почти любого из них может возникнуть необходимость возврата к предыдущему. Так, при идентификации активов может оказаться, что выбранные границы анализа следует расширить, а степень детализации – увеличить. Особенно труден первичный анализ, когда многократные возвраты к началу неизбежны.

4. Программы безопасности верхнего и процедурного уровня

4.6. Основные этапы управления рисками

Этапы, предшествующие анализу угроз, можно считать подготовительными, поскольку, строго говоря, они напрямую с рисками не связаны. Риск появляется там, где есть угрозы.

Краткий перечень наиболее распространённых угроз был рассмотрен нами ранее. К сожалению, на практике угроз гораздо больше, причём далеко не все из них носят компьютерный характер. Так, вполне реальной угрозой является наличие мышей и тараканов в занимаемых организацией помещениях. Первые могут повредить кабели, вторые вызвать короткое замыкание. Как правило, наличие той или иной угрозы является следствием пробелов в защите информационной системы, которые, в свою очередь, объясняются отсутствием некоторых сервисов безопасности или недостатками в реализующих их защитных механизмах. Опасность погрязания кабелей возникает не просто там, где есть мыши, она связана с отсутствием или недостаточной прочностью защитной оболочки.

Первый шаг в анализе угроз – их идентификация. Рассматриваемые виды угроз следует выбирать исходя из соображений здравого смысла (исключая, например, землетрясения, однако не забывая о возможности захвата организации террористами), но в пределах выбранных видов провести максимально подробный анализ.

4. Программы безопасности верхнего и процедурного уровня

4.6. Основные этапы управления рисками

Целесообразно выявлять не только сами угрозы, но и источники их возникновения – это поможет в выборе дополнительных средств защиты. Например, нелегальный вход в систему может стать следствием воспроизведения начального диалога, подбора пароля или подключения к сети неавторизованного оборудования. Очевидно, для противодействия каждому из перечисленных способов нелегального входа нужны свои механизмы безопасности. После идентификации угрозы необходимо оценить вероятность её осуществления. Допустимо использовать при этом трёхбалльную шкалу (низкая (1), средняя (2) и высокая (3) вероятности).

Кроме вероятности осуществления важен размер потенциального ущерба. Например, пожары бывают нечасто, но ущерб от каждого из них, как правило, велик. Тяжесть ущерба также можно оценить по трёхбалльной шкале.

Оценивая размер ущерба, необходимо иметь в виду не только непосредственные расходы на замену оборудования или восстановление информации, но и более отдалённые, такие как подрыв репутации, ослабление позиций на рынке и т.п. Пусть, например, в результате дефектов в управлении доступом к бухгалтерской информации сотрудники получили возможность корректировать данные о собственной заработной плате. Следствием такого состояния дел может стать не только перерасход бюджетных или корпоративных

4. Программы безопасности верхнего и процедурного уровня

4.6. Основные этапы управления рисками

Уязвимые места обладают свойством притягивать к себе не только злоумышленников, но и сравнительно честных людей. Не всякий устоит перед искушением немного увеличить свою зарплату, если есть уверенность, что это сойдёт с рук. Поэтому, оценивая вероятность осуществления угроз, целесообразно исходить не только из среднестатистических данных, но учитывать также специфику конкретных информационных систем. Если в подвале дома, занимаемого организацией, располагается сауна, а сам дом имеет деревянные перекрытия, то вероятность пожара, к сожалению, оказывается существенно выше средней.

После того как накоплены исходные данные и оценена степень неопределённости, можно переходить к обработке информации, то есть собственно к оценке рисков. Вполне допустимо применить такой простой метод, как умножение вероятности осуществления угрозы на предполагаемый ущерб. Если для вероятности и ущерба использовать трёхбалльную шкалу, то возможных произведений будет шесть: 1, 2, 3, 4, 6 и 9. Первые два результата можно отнести к низкому риску, третий и четвёртый – к среднему, два последних – к высокому, после чего появляется возможность снова привести их к трёхбалльной шкале. По этой шкале и следует оценивать приемлемость рисков. Правда, граничные случаи, когда вычисленная величина совпадает с приемлемой, целесообразно рассматривать более тщательно из-за

4. Программы безопасности верхнего и процедурного уровня

4.6. Основные этапы управления рисками

Если какие-либо риски оказались недопустимо высокими, необходимо их нейтрализовать, реализовав дополнительные меры защиты. Как правило, для ликвидации или нейтрализации уязвимого места, сделавшего угрозу реальной, существует несколько механизмов безопасности, различных по эффективности и стоимости. Например, если велика вероятность нелегального входа в систему, можно потребовать, чтобы пользователи выбирали длинные пароли (скажем, не менее восьми символов), задействовать программу генерации паролей или закупить интегрированную систему аутентификации на основе интеллектуальных карт. Если есть вероятность умышленного повреждения сервера баз данных, что может иметь серьёзные последствия, можно врезать замок в дверь серверной комнаты или поставить около каждого сервера по охраннику.

Оценивая стоимость мер защиты, приходится, разумеется, учитывать не только прямые расходы на закупку оборудования и/или программ, но и расходы на внедрение новинки и, в частности, обучение и переподготовку персонала. Эту стоимость также можно оценить по трёхбалльной шкале и затем сопоставить её с разностью между вычисленным и допустимым риском. Если по этому показателю новое средство оказывается экономически выгодным, его можно взять на заметку (подходящих средств, вероятно, будет несколько). Однако если средство окажется дорогим, его не следует сразу отбрасывать, памятуя о приближённости расчётов.

4. Программы безопасности верхнего и процедурного уровня

4.6. Основные этапы управления рисками

Выбирая подходящий способ защиты, целесообразно учитывать возможность экранирования одним механизмом обеспечения безопасности сразу нескольких прикладных сервисов. Так поступили в Массачусетском технологическом институте, защитив несколько тысяч компьютеров сервером аутентификации Kerberos.

Важным обстоятельством является совместимость нового средства со сложившейся организационной и аппаратно-программной структурой, с традициями организации. Меры безопасности, как правило, носят недружественный характер, что может отрицательно сказаться на энтузиазме сотрудников. Порой сохранение духа открытости важнее минимизации материальных потерь. Впрочем, такого рода ориентиры должны быть расставлены в политике безопасности верхнего уровня.

Можно представить себе ситуацию, когда для нейтрализации риска не существует эффективных и приемлемых по цене мер. Например, компания, базирующаяся в сейсмически опасной зоне, не всегда может позволить себе строительство защищённой штаб-квартиры. В таком случае приходится поднимать планку приемлемого риска и переносить центр тяжести на смягчение последствий и выработку планов восстановления после аварий, стихийных бедствий и иных происшествий. Продолжая пример с сейсмоопасностью, можно рекомендовать регулярное тиражирование данных в другой город и овладение

4. Программы безопасности верхнего и процедурного уровня

4.6. Основные этапы управления рисками

Как и всякую иную деятельность, реализацию и проверку новых регуляторов безопасности следует предварительно планировать. В плане необходимо учесть наличие финансовых средств и сроки обучения персонала. Если речь идёт о программно-техническом механизме защиты, нужно составить план тестирования (автономного и комплексного).

Когда намеченные меры приняты, необходимо проверить их действенность, то есть убедиться, что остаточные риски стали приемлемыми. Если это на самом деле так, значит, можно спокойно намечать дату ближайшей переоценки. В противном случае придётся проанализировать допущенные ошибки и провести повторный сеанс управления рисками немедленно.

4. Программы безопасности верхнего и процедурного уровня

4.7. Управление рисками при проектировании систем безопасности. Анализ рисков

Целью анализа рисков является оценка угроз и уязвимостей, определение комплекса контрмер, обеспечивающего достаточный уровень защищённости информационной системы. Существуют различные подходы к оценке рисков, выбор которых зависит от уровня требований, предъявляемых в организации к режиму информационной безопасности.

Цель процесса оценивания рисков состоит в определении характеристик рисков информационной системе и её ресурсам. На основе таких данных могут быть выбраны необходимые средства защиты. При оценивании рисков учитываются многие факторы: ценность ресурсов, оценки значимости угроз, уязвимостей, эффективность существующих и планируемых средств защиты и многое другое.

Основные подходы к анализу рисков

В настоящее время используются два подхода к анализу рисков. Их выбор зависит от оценки собственниками ценности своих информационных ресурсов и возможных последствий нарушения режима информационной безопасности. В простейшем случае собственники информационных ресурсов могут не оценивать эти параметры.

4. Программы безопасности верхнего и процедурного уровня

4.7. Управление рисками при проектировании систем безопасности. Анализ рисков

Неявно предполагается, что ценность защищаемых ресурсов с точки зрения организации не является чрезмерно высокой. В этом случае анализ рисков производится по упрощённой схеме: рассматривается стандартный набор наиболее распространённых угроз безопасности без оценки их вероятности и обеспечивается минимальный или базовый уровень ИБ.

Обычной областью использования этого уровня являются типовые проектные решения. Существует ряд стандартов и спецификаций, в которых рассматривается минимальный (типовой) набор наиболее вероятных угроз, таких как вирусы, сбои оборудования, несанкционированный доступ и т. д. Для нейтрализации этих угроз обязательно должны быть приняты контрмеры вне зависимости от вероятности их осуществления и уязвимости ресурсов. Таким образом, характеристики угроз на базовом уровне рассматривать не обязательно.

Полный вариант анализа рисков применяется в случае повышенных требований в области ИБ. В отличие от базового варианта в том или ином виде производится оценка ценности ресурсов, характеристик рисков и уязвимостей ресурсов. Как правило, проводится анализ стоимость/эффективность нескольких вариантов защиты.

4. Программы безопасности верхнего и процедурного уровня

4.7. Управление рисками при проектировании систем безопасности. Анализ рисков

Таким образом, при проведении полного анализа рисков необходимо:

- определить ценность ресурсов;
- к стандартному набору добавить список угроз, актуальных для исследуемой информационной системы;
- оценить вероятность угроз;
- определить уязвимость ресурсов;
- предложить решение, обеспечивающее необходимый уровень ИБ.

4. Программы безопасности верхнего и процедурного уровня

4.8. Анализ рисков в информационных системах с повышенными требованиями к безопасности

При выполнении полного анализа рисков приходится решать ряд сложных проблем:

- Как определить ценность ресурсов?
- Как составить полный список угроз ИБ и оценить их параметры?
- Как правильно выбрать контрмеры и оценить их эффективность?

Процесс оценивания рисков содержит несколько этапов:

- идентификация ресурса и оценивание его количественных показателей или определение потенциального негативного воздействия на бизнес;
- оценивание угроз;
- оценивание уязвимостей;
- оценивание существующих и предполагаемых средств обеспечения информационной безопасности;
- оценивание рисков.

На основе оценивания рисков выбираются средства, обеспечивающие режим ИБ. Ресурсы, значимые для бизнеса и имеющие определённую степень уязвимости, подвергаются риску, если по отношению к ним существует какая-либо угроза. При оценивании рисков учитываются потенциальное негативное воздействие от нежелательных происшествий и показатели значимости рассматриваемых уязвимостей и угроз для них.

4. Программы безопасности верхнего и процедурного уровня

4.8. Анализ рисков в информационных системах с повышенными требованиями к безопасности

Риск характеризует опасность, которой может подвергаться система и использующая её организация.

Степень риска зависит:

- показателей ценности ресурсов;
- вероятности реализации угроз;
- простоты использования уязвимости при возникновении угроз;
- существующих или планируемых к внедрению средств обеспечения ИБ, которые уменьшают уязвимости, сокращают вероятность возникновения угроз и негативных воздействий.

Определение ценности ресурсов

Важным шагом при анализе рисков является стадия оценки ценности информации. (рис. 7.2) .

4. Программы безопасности верхнего и процедурного уровня

4.8. Анализ рисков в информационных системах с повышенными требованиями к безопасности

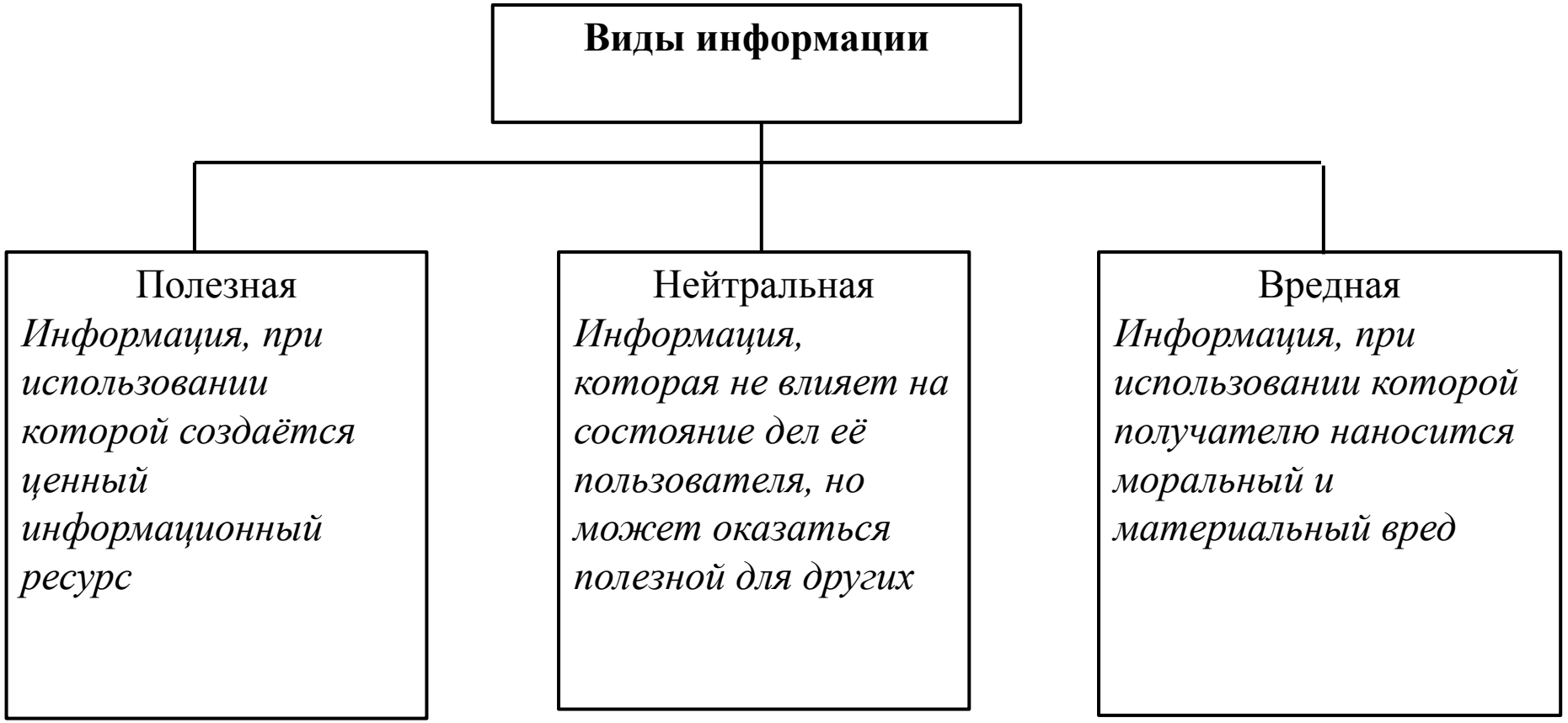

Рис. 7.2. Виды информации с позиции ценности

4. Программы безопасности верхнего и процедурного уровня

4.8. Анализ рисков в информационных системах с повышенными требованиями к безопасности

Ресурсы обычно подразделяются на несколько классов, например, физические, программные и данные. Для каждого класса должна существовать своя методика оценки ценности элементов.

Для оценки ценности ресурсов выбирается подходящая система критериев. Критерии должны позволять описать потенциальный ущерб, связанный с нарушением конфиденциальности, целостности, доступности.

Ценность физических ресурсов оценивается с точки зрения стоимости их замены или восстановления работоспособности. Эти стоимостные величины затем преобразуются в качественную шкалу, которая используется также для информационных ресурсов. Программные ресурсы оцениваются тем же способом, что и физические, на основе определения затрат на их приобретение или восстановление.

Если для информационного ресурса существуют особенные требования к конфиденциальности или целостности (например, исходный текст имеет высокую коммерческую ценность), то оценка этого ресурса производится по той же схеме, то есть в стоимостном выражении.

4. Программы безопасности верхнего и процедурного уровня

4.8. Анализ рисков в информационных системах с повышенными требованиями к безопасности

Кроме критериев, учитывающих финансовые потери, в коммерческих организациях могут присутствовать критерии, отражающие следующее:

- ущерб репутации организации;
- неприятности, связанные с нарушением действующего законодательства;
- ущерб для здоровья персонала;
- ущерб, связанный с разглашением персональных данных отдельных лиц;
- финансовые потери от разглашения информации;
- финансовые потери, связанные с восстановлением ресурсов;
- потери, связанные с невозможностью выполнения обязательств;
- ущерб от дезорганизации деятельности.

Могут использоваться и другие критерии, в зависимости от профиля организации. К примеру, в правительственных учреждениях могут добавляться критерии, отражающие такие области, как национальная безопасность и международные отношения.

4. Программы безопасности верхнего и процедурного уровня

4.8. Анализ рисков в информационных системах с повышенными требованиями к безопасности

Оценка характеристик факторов риска

Ресурсы должны быть проанализированы с точки зрения оценки воздействия возможных атак (спланированных действий внутренних или внешних злоумышленников) и различных нежелательных событий естественного происхождения. Такие потенциально возможные события будем называть угрозами безопасности.

Кроме того, необходимо идентифицировать уязвимости – слабости в системе защиты, которые делают возможным реализацию угроз.

Для того чтобы конкретизировать вероятность реализации угрозы, рассматривается некоторый отрезок времени, в течение которого предполагается защищать ресурс.

Вероятность того, что угроза реализуется, определяется следующими факторами:

- привлекательностью ресурса (этот показатель учитывается при рассмотрении угрозы умышленного воздействия со стороны человека);
- возможностью использования ресурса для получения дохода (показатель учитывается при рассмотрении угрозы умышленного воздействия со стороны

4. Программы безопасности верхнего и процедурного уровня

4.8. Анализ рисков в информационных системах с повышенными требованиями к безопасности

В настоящее время известно множество методов оценивания угроз, большинство из которых построены на использовании таблиц. Такие методы сравнительно просты в использовании и достаточно эффективны. Однако не стоит говорить о «лучшем» методе, так как в различных случаях они будут разными. Важно из имеющегося многообразия методов выбрать именно тот, который обеспечивал бы воспроизводимые результаты для данной организации.

Ранжирование угроз

В матрице или таблице можно наглядно отразить связь факторов негативного воздействия (показателей ресурсов) и вероятностей реализации угрозы с учётом показателей уязвимостей (табл. 7.1).

Дескриптор угрозы (a)	Показатель негативного воздействия (ресурса)(b)	Вероятность реализации угрозы (c)	Показатель риска (d)	Ранг угрозы (e)
Угроза A	5	2	10	2
Угроза B	2	4	8	3
Угроза C	3	5	15	1
Угроза D	1	3	3	5
Угроза E	4	1	4	4
Угроза F	2	4	8	3

4. Программы безопасности верхнего и процедурного уровня

4.8. Анализ рисков в информационных системах с повышенными требованиями к безопасности

На первом шаге оценивается негативное воздействие (показатель ресурса) по заранее определённой шкале, например, от 1 до 5, для каждого ресурса, которому угрожает опасность (колонка b в таблице).

На втором – по заранее заданной шкале, например, от 1 до 5, оценивается вероятность реализации каждой угрозы.

На третьем шаге вычисляется показатель риска. В простейшем варианте методики это делается путём умножения ($b \cdot c$). Однако необходимо помнить, что операция умножения определена для количественных шкал. Для ранговых (качественных) шкал измерения, каковыми являются показатель негативного воздействия и вероятность реализации угрозы, к примеру, совсем не обязательно, что показатель риска, соответствующий ситуации $b=1$, $c=3$, будет эквивалентен $b=3$, $c=1$. Соответственно, должна быть разработана методика оценивания показателей рисков применительно к конкретной организации.

На четвёртом шаге угрозы ранжируются по значениям их фактора риска.
В рассматриваемом примере для обозначения наименьшего негативного воздействия и наименьшей вероятности реализации выбран показатель 1.
Данная процедура позволяет сравнивать и ранжировать по приоритету угрозы с различными негативными воздействиями и вероятностями реализации.

4. Программы безопасности верхнего и процедурного уровня

4.8. Анализ рисков в информационных системах с повышенными требованиями к безопасности

Оценивание показателей частоты повторяемости и возможного ущерба от риска

Рассмотрим пример оценки негативного воздействия от нежелательных происшествий.

Каждому ресурсу присваивается определённое значение, соответствующее потенциальному ущербу от воздействия угрозы. Такие показатели присваиваются ресурсу по отношению ко всем возможным угрозам.

Далее оценивается показатель частоты повторяемости. Частота зависит от вероятности возникновения угрозы и простоты использования уязвимости. Показатель частоты является субъективной мерой возможности реализации угрозы и оценивается, как правило, в качественных шкалах. Примером является табл. 7.2, где заданы субъективные частоты реализации события в шкале 0 (крайне редко) – 4 (очень часто) для разных уровней угроз и уязвимостей (Н, С, В – низкий, средний, высокий уровень уязвимости). Далее определяется субъективная шкала рисков в зависимости от показателя ценности ресурса и частоты, пример приведён в табл. 7.3 (0 – минимальный риск, 8 – максимальный риск). Эти значения должны отражать позицию организации по отношению к рассматриваемым рискам.

4. Программы безопасности верхнего и процедурного уровня

4.8. Анализ рисков в информационных системах с повышенными требованиями к безопасности

Таблица 7.2. Уровни угрозы

Уровень угрозы								
Низкий			Средний			Высокий		
Уровни уязвимости	Уровни уязвимости	Уровни уязвимости	Уровни уязвимости	Уровни уязвимости	Уровни уязвимости	Уровни уязвимости	Уровни уязвимости	Уровни уязвимости
Н	С	В	Н	С	В	Н	С	В
0	1	2	1	2	3	2	3	4

Таблица 7.3. Субъективные

Показатель ресурса	**Показатель частоты**				
	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	5
2	2	3	4	5	6
3	3	4	5	6	7
4	4	5	6	7	8

4. Программы безопасности верхнего и процедурного уровня

4.8. Анализ рисков в информационных системах с повышенными требованиями к безопасности

Оценивание уровней рисков

Рассмотрим пример метода, построенного на использовании таблиц и учитывающего только стоимостные характеристики ресурсов.

Ценность физических ресурсов оценивается с точки зрения стоимости их замены или восстановления работоспособности (то есть количественных показателей). Эти стоимостные величины затем преобразуются в качественную шкалу, которая используется также для информационных ресурсов. Программные ресурсы оцениваются тем же способом, что и физические, исходя из затрат на их приобретение или восстановление.

Если для информационного ресурса существуют особенные требования к конфиденциальности или целостности (например, если исходный текст имеет высокую коммерческую ценность), то оценка этого ресурса производится по той же схеме, то есть в стоимостном выражении.

4. Программы безопасности верхнего и процедурного уровня

4.8. Анализ рисков в информационных системах с повышенными требованиями к безопасности

Количественные показатели информационных ресурсов оцениваются на основании опросов сотрудников компании (владельцев информации) – тех, кто может оценить ценность информации, определить её характеристики и степень критичности. На основе результатов опроса производится оценивание показателей и степени критичности информационных ресурсов для наихудшего варианта развития событий. Рассматривается потенциальное воздействие на бизнес-процесс при возможном несанкционированном ознакомлении с информацией, изменении информации, отказе от выполнения обработки информации, недоступности на различные сроки и разрушении.

Далее разрабатывается система показателей в балльных шкалах (пример – четырёхпольная шкала (от 0 до 4), приведённая ниже). Таким образом, количественные показатели используются там, где это допустимо и оправданно, а качественные – там, где количественные оценки невозможны, например, при угрозе человеческой жизни.

По каждой группе ресурсов, связанной с данной угрозой, оценивается уровень последней (вероятность реализации) и степень уязвимости (лёгкость, с которой реализованная угроза способна привести к негативному воздействию). Оценивание производится в качественных шкалах.

4. Программы безопасности верхнего и процедурного уровня

4.8. Анализ рисков в информационных системах с повышенными требованиями к безопасности

Например, уровень угроз и уровень уязвимостей можно оценить по шкале «высокий-средний-низкий». Информацию собирают, опрашивая сотрудников, занимающихся техническими вопросами, и анализируя документацию.

Пример.

Уровни риска определяются тремя параметрами: ценностью ресурса, уровнями угрозы и уязвимости.

Каждому значению уровня риска должно быть поставлено в соответствие описание, позволяющее однозначно его трактовать разным людям и понимать, где проходит граница между значениями.

4. Программы безопасности верхнего и процедурного уровня

4.8. Анализ рисков в информационных системах с повышенными требованиями к безопасности

Например, показатель риска измеряется в шкале от 0 до 8 со следующими определениями уровней риска:

1 – риск практически отсутствует. Теоретически возможны ситуации, при которых событие наступает, но на практике это случается редко, а потенциальный ущерб сравнительно невелик.

2 – риск очень мал. События подобного рода случались достаточно редко, кроме того, негативные последствия сравнительно невелики.

.....

8 – риск очень велик. Событие скорее всего наступит, и последствия будут чрезвычайно тяжёлыми.

Пример матрицы приводится в табл. 7.4.

Таблица 7.4. Пример матрицы

Ценность ресурса	**Уровень угрозы**								
	Низкий			Средний			Высокий		
	Уровни уязвимостей			Уровни уязвимостей			Уровни уязвимостей		
	Н	С	В	Н	С	В	Н	С	В
0	0	1	2	1	2	3	2	3	4
1	1	2	3	2	3	4	3	4	5
2	2	3	4	3	4	5	4	5	6
3	3	4	5	4	5	6	5	6	7
4	4	5	6	5	6	7	6	7	8

4. Программы безопасности верхнего и процедурного уровня

4.8. Анализ рисков в информационных системах с повышенными требованиями к безопасности

Для каждого ресурса рассматриваются относящиеся к нему уязвимые места и соответствующие им угрозы. Если уязвимость существует, но нет связанной с ней угрозы или существует угроза, не связанная с какими-либо уязвимыми местами, то в такой ситуации рисков нет. Однако надо иметь в виду, что в дальнейшем ситуация может измениться.

Каждая строка в матрице определяется показателем ресурса, а каждый столбец – степенью опасности угрозы и уязвимости. Например, ресурс имеет ценность 3, угроза имеет степень «высокая», а уязвимость – степень «низкая». Показатель риска в данном случае будет равен 5. В случае, когда ресурс имеет ценность 2, например, для модификации, уровень угрозы низкий, а уязвимости, напротив, высокий, показатель риска окажется равен 4.

Размер матрицы, учитывающей количество степеней угроз и уязвимостей, категорий ресурсов, может быть другим и определяется конкретной организацией.

После того как оценивание рисков было выполнено первый раз, его результаты обычно сохраняют в базе данных. В дальнейшем проводить повторное оценивание будет значительно легче.

Разделение рисков на приемлемые и не приемлемые

Другой способ оценивания рисков состоит в разделении их только на приемлемые и не приемлемые. Подход основывается на том, что количественные показатели рисков используются только для их упорядочивания и определения первоочередных действий. Но этого можно достичь и с меньшими затратами.

Матрица, используемая в данном подходе, содержит не числа, а только символы Д (риск допустим) и Н (риск не допустим). Например, может быть использована матрица, представленная в табл. 7.5.

Показатель ресурса	Показатель частоты				
	0	1	2	3	4
0	Д	Д	Д	Д	Н
1	Д	Д	Д	Н	Н
2	Д	Д	Н	Н	Н
3	Д	Н	Н	Н	Н
4	Н	Н	Н	Н	Н

4. Программы безопасности верхнего и процедурного уровня

4.8. Анализ рисков в информационных системах с повышенными требованиями к безопасности

Разделение рисков на приемлемые и не приемлемые

Другой способ оценивания рисков состоит в разделении их только на приемлемые и не приемлемые. Подход основывается на том, что количественные показатели рисков используются только для их упорядочивания и определения первоочередных действий. Но этого можно достичь и с меньшими затратами.

Матрица, используемая в данном подходе, содержит не числа, а только символы Д (риск допустим) и Н (риск не допустим). Например, может быть использована матрица, представленная в табл. 7.5.

Показатель ресурса	Показатель частоты				
	0	1	2	3	4
0	Д	Д	Д	Д	Н
1	Д	Д	Д	Н	Н
2	Д	Д	Н	Н	Н
3	Д	Н	Н	Н	Н
4	Н	Н	Н	Н	Н

Вопрос о том, как провести границу между приемлемыми и не приемлемыми рисками, остаётся на усмотрении пользователя

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

Перейдём к рассмотрению мер безопасности, которые ориентированы на людей, а не на технические средства. Именно люди формируют режим информационной безопасности, и они же оказываются главной угрозой, поэтому "человеческий фактор" заслуживает особого внимания.

В российских компаниях накоплен богатый опыт регламентирования и реализации процедурных (организационных) мер, однако дело в том, что они пришли из "докомпьютерного" прошлого, поэтому требуют переоценки.

Следует осознать ту степень зависимости от компьютерной обработки данных, в которую попало современное общество. Без всякого преувеличения можно сказать, что необходима информационная гражданская оборона. Спокойно, без нагнетания страстей нужно разъяснять обществу не только преимущества, но и опасности, связанные с использованием информационных технологий. Акцент следует делать не на военной или криминальной стороне дела, а на гражданских аспектах, связанных с поддержанием нормального функционирования аппаратного и программного обеспечения, то есть концентрироваться на вопросах доступности и целостности данных.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

На процедурном уровне можно выделить следующие классы мер:
- управление персоналом;
- физическая защита;
- поддержание работоспособности;
- реагирование на нарушения режима безопасности;
- планирование восстановительных работ.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.1. Управление персоналом

Управление персоналом начинается с приёма нового сотрудника на работу и даже раньше — с составления описания должности. Уже на данном этапе желательно подключить к работе специалиста по информационной безопасности для определения компьютерных привилегий, ассоциируемых с должностью. Существует два общих принципа, которые следует иметь в виду:

- разделение обязанностей;
- минимизация привилегий.

Принцип разделения обязанностей предписывает так распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс. Например, нежелательна ситуация, когда крупные платежи от имени организации выполняет один человек. Надёжнее поручить одному сотруднику оформление заявок на подобные платежи, а другому – заверять эти заявки. Другой пример – процедурные ограничения действий суперпользователя. Можно искусственно «расщепить» пароль суперпользователя, сообщив первую его часть одному сотруднику, а вторую – другому. Тогда критически важные действия по администрированию ИС они смогут выполнить только вдвоём, что снижает вероятность ошибок и злоупотреблений.

5. Процедурный уровень информационной безопасности Основные классы мер процедурного уровня

5.1. Управление персоналом

Принцип минимизации привилегий предписывает выделять пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей. Назначение этого принципа очевидно – уменьшить ущерб от случайных или умышленных некорректных действий.

Предварительное составление описания должности позволяет оценить её критичность и спланировать процедуру проверки и отбора кандидатов. Чем ответственнее должность, тем тщательнее нужно проверять кандидатов: навести о них справки, быть может, побеседовать с бывшими сослуживцами и т. д. Подобная процедура может быть длительной и дорогой, поэтому нет смысла дополнительно усложнять её. В то же время неразумно и совсем отказываться от предварительной проверки, чтобы случайно не принять на работу человека с уголовным прошлым или психическим заболеванием.

Когда кандидат определён, он, вероятно, должен пройти обучение; по крайней мере, его следует подробно ознакомить со служебными обязанностями, а также с нормами и процедурами информационной безопасности. Желательно, чтобы меры безопасности были им усвоены до вступления в должность и до заведения его системного счета с входным именем, паролем и привилегиями.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.1. Управление персоналом

С момента заведения системного счета начинается его администрирование, а также протоколирование и анализ действий пользователя. Постепенно изменяется окружение, в котором работает пользователь, его служебные обязанности и т.п. Все это требует соответствующего изменения привилегий. Техническую сложность представляют временные перемещения пользователя, выполнение им обязанностей взамен сотрудника, ушедшего в отпуск, и иные обстоятельства, когда полномочия нужно сначала предоставить, а через некоторое время взять обратно. В такие периоды профиль активности пользователя резко меняется, что создаёт трудности при выявлении подозрительных ситуаций. Определённую аккуратность следует соблюдать и при выдаче новых постоянных полномочий, не забывая ликвидировать старые права доступа.

Ликвидация системного счета пользователя, особенно в случае конфликта между сотрудником и организацией, должна производиться максимально оперативно (в идеале – одновременно с извещением о наказании или увольнении). Возможно и физическое ограничение доступа к рабочему месту. Разумеется, если сотрудник увольняется, у него нужно принять все его компьютерное хозяйство и, в частности, криптографические ключи, если использовались средства шифрования.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.1. Управление персоналом

К управлению сотрудниками примыкает администрирование лиц, работающих по контракту (например, специалистов фирмы-поставщика, помогающих запустить новую систему). В соответствии с принципом минимизации привилегий им нужно выделить ровно столько прав, сколько необходимо, и изъять эти права сразу по окончании контракта.

Проблема, однако, состоит в том, что на начальном этапе внедрения «внешние» сотрудники будут администрировать «местных», а не наоборот. Здесь на первый план выходит квалификация персонала организации, его способность быстро обучаться, а также оперативное проведение учебных курсов. Важны и принципы выбора деловых партнёров.

Иногда внешние организации принимают на обслуживание и администрирование ответственные компоненты компьютерной системы, например, сетевое оборудование. Нередко администрирование выполняется в удалённом режиме. Вообще говоря, это создаёт в системе дополнительные уязвимые места, которые необходимо компенсировать усиленным контролем средств удалённого доступа или, опять-таки, обучением собственных сотрудников.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.1. Управление персоналом

Мы видим, что проблема обучения – одна из основных с точки зрения информационной безопасности. Если сотрудник не знаком с политикой безопасности своей организации, он не может стремиться к достижению сформулированных в ней целей. Не зная мер безопасности, он не сможет их соблюдать.

Напротив, если сотрудник знает, что его действия протоколируются, он, возможно, воздержится от нарушений.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.2. Физическая защита

Безопасность информационной системы зависит от окружения, в котором она функционирует. Необходимо принять меры для защиты зданий и прилегающей территории, поддерживающей инфраструктуры, вычислительной техники, носителей данных.

Основной принцип физической защиты, соблюдение которого следует постоянно контролировать, формулируется как «непрерывность защиты в пространстве и времени». Ранее мы рассматривали понятие окна опасности. Для физической защиты таких окон быть не должно.

Мы кратко рассмотрим следующие направления физической защиты:
- физическое управление доступом;
- противопожарные меры;
- защита поддерживающей инфраструктуры;
- защита от перехвата данных;
- защита мобильных систем.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.2. Физическая защита

Меры физического управления доступом позволяют контролировать и при необходимости ограничивать вход и выход сотрудников и посетителей. Контролироваться может все здание организации, а также отдельные помещения, например, те, где расположены серверы, коммуникационная аппаратура и т.п.

При проектировании и реализации мер физического управления доступом целесообразно применять объектный подход. Во-первых, определяется периметр безопасности, ограничивающий контролируемую территорию. На этом уровне детализации важно продумать внешний интерфейс организации – порядок входа/выхода штатных сотрудников и посетителей, вноса/выноса техники. Все, что не входит во внешний интерфейс, должно быть инкапсулировано, то есть защищено от нелегальных проникновений.

Во-вторых, производится декомпозиция контролируемой территории, выделяются (под)объекты и связи (проходы) между ними. При такой более глубокой детализации следует выделить среди подобъектов наиболее критичные с точки зрения безопасности и обеспечить им повышенное внимание.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.2. Физическая защита

Декомпозиция должна быть семантически оправданной, обеспечивающей разграничение разнородных сущностей, таких как оборудование разных владельцев или персонал, работающий с данными разной степени критичности. Важно сделать так, чтобы посетители, по возможности, не имели непосредственного доступа к компьютерам, или, в крайнем случае, позаботиться о том, чтобы от окон и дверей не просматривались экраны мониторов и принтеры. Необходимо, чтобы посетителей по внешнему виду можно было отличить от сотрудников. Если отличие состоит в том, что посетителям выдаются идентификационные карточки, а сотрудники ходят «без опознавательных знаков», злоумышленнику достаточно снять карточку, чтобы его считали "своим". Очевидно, соответствующие карточки нужно выдавать всем.

Средства физического управления доступом известны давно. Это охрана, двери с замками, перегородки, телекамеры, датчики движения и многое другое. Для выбора оптимального (по критерию стоимость/эффективность) средства целесообразно провести анализ рисков (к этому мы ещё вернёмся). Кроме того, есть смысл периодически отслеживать появление технических новинок в данной области, стараясь максимально автоматизировать физическую защиту.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.2. Физическая защита

Профессия пожарника – одна из древнейших, но пожары по-прежнему случаются и наносят большой ущерб. Мы не собираемся цитировать параграфы противопожарных инструкций или изобретать новые методы борьбы с огнём – на это есть профессионалы.

Отметим лишь необходимость установки противопожарной сигнализации и автоматических средств пожаротушения. Обратим также внимание на то, что защитные меры могут создавать новые слабые места. Если на работу взят новый охранник, это, вероятно, улучшает физическое управление доступом. Если же он по ночам курит и пьёт, то ввиду повышенной пожароопасности подобная мера зашиты может только навредить.

К поддерживающей инфраструктуре можно отнести системы электро-, водо- и теплоснабжения, кондиционеры и средства коммуникаций. В принципе, к ним применимы те же требования целостности и доступности, что и к информационным системам. Для обеспечения целостности нужно защищать оборудование от краж и повреждений. Для поддержания доступности следует выбирать оборудование с максимальным временем наработки на отказ, дублировать ответственные узлы и всегда иметь под рукой запчасти.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.2. Физическая защита

Отдельную проблему составляют аварии водопровода. Они происходят нечасто, но могут нанести огромный ущерб. При размещении компьютеров необходимо принять во внимание расположение водопроводных и канализационных труб и постараться держаться от них подальше. Сотрудники должны знать, куда следует обращаться при обнаружении протечек.

Перехват данных (о чём мы уже писали) может осуществляться самыми разными способами. Злоумышленник может подсматривать за экраном монитора, читать пакеты, передаваемые по сети, производить анализ побочных электромагнитных излучений и наводок (ПЭМИН) и т.д. Остаётся уповать на повсеместное использование криптографии (что, впрочем, сопряжено у нас в стране со множеством технических и законодательных проблем), стараться максимально расширить контролируемую территорию, разместившись в тихом особнячке, поодаль от других домов, пытаться держать под контролем линии связи (например, заключать их в надувную оболочку с обнаружением прокалывания), но самое разумное, вероятно, – постараться осознать, что для коммерческих систем обеспечение конфиденциальности является все-таки не главной задачей.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.2. Физическая защита

Мобильные и портативные компьютеры – заманчивый объект кражи. Их часто оставляют без присмотра, в автомобиле или на работе, и похитить такой компьютер совсем несложно. То и дело средства массовой информации сообщают о том, что какой-нибудь офицер английской разведки или американский военный лишился таким образом движимого имущества. Мы настоятельно рекомендуем шифровать данные на жест-ких дисках таких компьютеров.

Вообще говоря, при выборе средств физической защиты следует производить анализ рисков. Так, принимая решение о закупке источника бесперебойного питания, необходимо учесть качество электропитания в здании, занимаемом организацией (впрочем, почти наверняка оно окажется плохим), характер и длительность сбоев электропитания, стоимость доступных источников и возможные потери от аварий (поломка техники, приостановка работы организации и т.п.). В то же время во многих случаях решения очевидны. Меры противопожарной безопасности обязательны для всех организаций. Стоимость реализации многих мер (например, установка обычного замка на дверь серверной комнаты) либо мала, либо хоть и заметна, но все же явно меньше, чем возможный ущерб. В частности, имеет смысл регулярно копировать большие базы данных.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.3. Поддержание работоспособности

Далее рассмотрим ряд рутинных мероприятий, направленных на поддержание работоспособности информационных систем. Именно здесь таится наибольшая опасность. Нечаянные ошибки системных администраторов и пользователей грозят повреждением аппаратуры, разрушением программ и данных; в лучшем случае они создают бреши в защите, которые делают возможной реализацию угроз.

Недооценка факторов безопасности в повседневной работе – «ахиллесова пята» многих организаций. Дорогие средства безопасности теряют смысл, если они плохо документированы, конфликтуют с другим программным обеспечением, а пароль системного администратора не менялся с момента установки.

Можно выделить следующие направления повседневной деятельности:
- поддержка пользователей;
- поддержка программного обеспечения;
- конфигурационное управление;
- резервное копирование;
- управление носителями;
- документирование;

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.3. Поддержание работоспособности

Поддержка пользователей подразумевает, прежде всего, консультирование и оказание помощи при решении разного рода проблем. Иногда в организациях создают для этой цели специальный справочный стол, но чаще от пользователей отбивается системный администратор. Очень важно в потоке вопросов уметь выявлять проблемы, связанные с информационной безопасностью. Так, многие трудности пользователей, работающих на персональных компьютерах, могут быть следствием заражения вирусами. Целесообразно фиксировать вопросы пользователей, чтобы выявлять их типичные ошибки и выпускать памятки с рекомендациями для распространённых ситуаций.

Поддержка программного обеспечения – одно из важнейших средств обеспечения целостности информации. Прежде всего, необходимо следить за тем, какое программное обеспечение установлено на компьютерах. Если пользователи будут устанавливать программы по своему усмотрению, это может привести к заражению вирусами, а также появлению утилит, действующих в обход защитных средств. Вполне вероятно также, что «самодеятельность» пользователей постепенно приведёт к хаосу на их компьютерах, а исправлять ситуацию придётся системному администратору.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.3. Поддержание работоспособности

Второй аспект поддержки программного обеспечения — контроль за отсутствием неавторизованного изменения программ и прав доступа к ним. Сюда же можно отнести поддержку эталонных копий программных систем. Обычно контроль достигается комбинированием средств физического и логического управления доступом, а также использованием утилит проверки и обеспечения целостности.

Конфигурационное управление позволяет контролировать и фиксировать изменения, вносимые в программную конфигурацию. Прежде всего, необходимо застраховаться от случайных или непродуманных модификаций, уметь как минимум возвращаться к прошлой работающей версии. Фиксация изменений позволит легко восстановить текущую версию после аварии.

Лучший способ уменьшить количество ошибок в рутинной работе – максимально автоматизировать её. Правы те «ленивые» программисты и системные администраторы, которые, окинув взглядом море однообразных задач, говорят: «Я ни за что не буду делать этого; я напишу программу, которая сделает все за меня». Автоматизация и безопасность зависят друг от друга; тот, кто заботится в первую очередь об облегчении своей задачи, на самом деле оптимальным образом формирует режим информационной безопасности.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.3. Поддержание работоспособности

Резервное копирование необходимо для восстановления программ и данных после аварий. И здесь целесообразно автоматизировать работу, как минимум сформировав компьютерное расписание создания полных и инкрементальных копий и как максимум – воспользовавшись соответствующими программными продуктами. Нужно также наладить размещение копий в безопасном месте, защищённом от несанкционированного доступа, пожаров, протечек, то есть от всего, что может привести к краже или повреждению носителей. Целесообразно иметь несколько экземпляров резервных копий и часть из них хранить вне территории организации, защищаясь таким образом от крупных аварий и аналогичных инцидентов.

Время от времени в тестовых целях следует проверять возможность восстановления информации с копий.

Управлять носителями необходимо для обеспечения физической защиты и учёта дискет, лент, печатных выдач и т.п. Управление носителями должно обеспечивать конфиденциальность, целостность и доступность информации, хранящейся вне компьютерных систем. Под физической защитой здесь понимается не только отражение попыток несанкционированного доступа, но и предохранение от вредных влияний окружающей среды (жары, холода, влаги, магнетизма). Управление носителями должно охватывать весь жизненный цикл от закупки до выведения из эксплуатации.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.3. Поддержание работоспособности

Документирование – неотъемлемая часть информационной безопасности. В виде документов оформляется почти все от политики безопасности до журнала учёта носителей. Важно, чтобы документация была актуальной, отражала именно текущее состояние дел, причём в непротиворечивом виде.

К хранению одних документов (содержащих, например, анализ уязвимых мест системы и угроз) применимы требования обеспечения конфиденциальности, к другим, таким как план восстановления после аварий, – требования целостности и доступности (в критической ситуации план необходимо найти и прочитать).

Регламентные работы очень серьёзная угроза безопасности. Сотрудник, осуществляющий регламентные работы, получает исключительный доступ к системе, и на практике очень трудно проконтролировать, какие именно действия он совершает. Здесь на первый план выходит степень доверия к тем, кто выполняет работу.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.4. Реагирование на нарушения режима безопасности

Программа безопасности, принятая организацией, должна предусматривать набор оперативных мероприятий, направленных на обнаружение и нейтрализацию нарушений режима информационной безопасности. Важно, чтобы в подобных случаях последовательность действий была спланирована заранее, поскольку меры нужно принимать срочные и скоординированные.

Реакция на нарушения режима безопасности преследует три главные цели:
- локализация инцидента и уменьшение наносимого вреда;
- выявление нарушителя;
- предупреждение повторных нарушений.

В организации должен быть человек, доступный 24 часа в сутки (лично, по телефону, пейджеру или электронной почте), который отвечает за реакцию на нарушения. Все должны знать координаты этого человека и обращаться к нему при первых признаках опасности. В общем, как при пожаре, нужно знать, куда звонить и что делать до приезда пожарной команды.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.4. Реагирование на нарушения режима безопасности

Важность быстрой и скоординированной реакции можно продемонстрировать на следующем примере. Пусть локальная сеть предприятия состоит из двух сегментов, администрируемых разными людьми. Далее, пусть в один из сегментов был внесён вирус. Почти наверняка через несколько минут (или, в крайнем случае, несколько десятков минут) вирус распространится и на другой сегмент. Значит, меры нужно принять немедленно. «Вычищать» вирус необходимо одновременно в обоих сегментах; в противном случае сегмент, восстановленный первым, заразится от другого, а затем вирус вернётся и во второй сегмент.

Нередко требование локализации инцидента и уменьшения наносимого вреда вступает в конфликт с желанием выявить нарушителя. В политике безопасности организации приоритеты должны быть расставлены заранее. Поскольку, как показывает практика, выявить злоумышленника очень сложно, на наш взгляд, в первую очередь, следует заботиться об уменьшении ущерба. Чтобы найти нарушителя, нужно заранее выяснить контактные координаты поставщика сетевых услуг и договориться с ним о самой возможности и порядке выполнения соответствующих действий.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.4. Реагирование на нарушения режима безопасности

Чтобы предотвратить повторные нарушения, необходимо анализировать каждый инцидент, выявлять причины, накапливать статистику.

Каковы источники вредоносного ПО?
Какие пользователи имеют обыкновение выбирать слабые пароли?

На подобные вопросы и должны дать ответ результаты анализа.

Необходимо отслеживать появление новых уязвимых мест и как можно быстрее ликвидировать ассоциированные с ними окна опасности. Кто-то в организации должен курировать этот процесс, принимать краткосрочные меры и корректировать программу безопасности для принятия долгосрочных мер.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.5. Планирование восстановительных работ

Ни одна организация не застрахована от серьёзных аварий, вызванных естественными причинами, действиями злоумышленника, халатностью или некомпетентностью. В то же время у каждой организации есть функции, которые руководство считает критически важными, они должны выполняться несмотря ни на что.

Планирование восстановительных работ позволяет подготовиться к авариям, уменьшить ущерб от них и сохранить способность к функционированию хотя бы в минимальном объёме.

Отметим, что меры информационной безопасности можно разделить на три группы, в зависимости от того, направлены ли они на предупреждение, обнаружение или ликвидацию последствий атак. Большинство мер носит предупредительный характер. Оперативный анализ регистрационной информации и некоторые аспекты реагирования на нарушения (так называемый активный аудит) служат для обнаружения и отражения атак.

Планирование восстановительных работ, очевидно, можно отнести к последней из трёх перечисленных групп.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.5. Планирование восстановительных работ

Процесс планирования восстановительных работ можно разделить на следующие этапы:

- выявление критически важных функций организации, установление приоритетов;
- идентификация ресурсов, необходимых для выполнения критически важных функций;
- определение перечня возможных аварий;
- разработка стратегии восстановительных работ;
- подготовка к реализации выбранной стратегии;
- проверка стратегии.

Планируя восстановительные работы, следует отдавать себе отчёт в том, что полностью сохранить функционирование организации не всегда возможно. Необходимо выявить критически важные функции, без которых организация теряет своё лицо, и даже среди критичных функций расставить приоритеты, чтобы как можно быстрее и с минимальными затратами возобновить работу после аварии.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.5. Планирование восстановительных работ

Идентифицируя ресурсы, необходимые для выполнения критически важных функций, следует помнить, что многие из них имеют некомпьютерный характер. На данном этапе желательно подключать к работе специалистов разного профиля, способных в совокупности охватить все аспекты проблемы.

Критичные ресурсы обычно относятся к одной из следующих категорий:
- персонал;
- информационная инфраструктура;
- физическая инфраструктура.

Составляя списки ответственных специалистов, следует учитывать, что некоторые из них могут непосредственно пострадать от аварии (например, от пожара), кто-то может находиться в состоянии стресса, часть сотрудников, возможно, будет лишена возможности попасть на работу (например, в случае массовых беспорядков). Желательно иметь некоторый резерв специалистов или заранее определить каналы, по которым можно на время привлечь дополнительный персонал.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.5. Планирование восстановительных работ

Информационная инфраструктура включает в себя следующие элементы:
- компьютеры;
- программы и данные;
- информационные сервисы внешних организаций;
- документацию.

Нужно подготовиться к тому, что на «запасном аэродроме», куда организация будет эвакуирована после аварии, аппаратная платформа может отличаться от исходной. Соответственно, следует продумать меры поддержания совместимости по программам и данным.

Среди внешних информационных сервисов для коммерческих организаций, вероятно, важнее всего получить оперативную информацию и связь с государственными службами, курирующими данный сектор экономики.

Документация важна хотя бы потому, что не вся информация, с которой работает организация, представлена в электронном виде. Скорее всего план восстановительных работ напечатан на бумаге.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.5. Планирование восстановительных работ

К физической инфраструктуре относятся здания, инженерные коммуникации, средства связи, оргтехника и многое другое. Компьютерная техника не может работать в плохих условиях, без стабильного электропитания и т.п.

Анализируя критичные ресурсы, целесообразно учесть временной профиль их использования. Большинство ресурсов требуются постоянно, но в некоторых нужда может возникать только в определённые периоды (например, в конце месяца или года при составлении отчёта).

При определении перечня возможных аварий нужно попытаться разработать их сценарии. Как будут развиваться события? Каковы могут оказаться масштабы бедствия? Что произойдёт с критичными ресурсами? Например, смогут ли сотрудники попасть на работу? Будут ли выведены из строя компьютеры? Возможны ли случаи саботажа? Будет ли работать связь? Пострадает ли здание организации? Можно ли будет найти и прочитать необходимые бумаги?

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.5. Планирование восстановительных работ

Стратегия восстановительных работ должна базироваться на наличных ресурсах и быть не слишком накладной для организации. При разработке стратегии целесообразно провести анализ рисков, которым подвергаются критичные функции, и попытаться выбрать наиболее экономичное решение.

Стратегия должна предусматривать не только работу по временной схеме, но и возвращение к нормальному функционированию.

Подготовка к реализации выбранной стратегии состоит в выработке плана действий в экстренных ситуациях и по их окончании, а также в обеспечении некоторой избыточности критичных ресурсов. Последнее возможно и без большого расхода средств, если заключить с одной или несколькими организациями соглашения о взаимной поддержке в случае аварий – те, кто не пострадал, предоставляют часть своих ресурсов во временное пользование менее удачливым партнёрам.

5. Процедурный уровень информационной безопасности
Основные классы мер процедурного уровня

5.5. Планирование восстановительных работ

Избыточность обеспечивается также мерами резервного копирования, хранением копий в нескольких местах, представлением информации в разных видах (на бумаге и в файлах) и т.д.

Имеет смысл заключить соглашение с поставщиками информационных услуг о первоочередном обслуживании в критических ситуациях или заключать соглашения с несколькими поставщиками. Правда, эти меры могут потребовать определённых расходов.

Проверка стратегии производится путём анализа подготовленного плана, принятых и намеченных мер.