Тема: Менеджмент коммуникаций и работ.

Вопрос 1: Менеджмент коммуникаций и работ.

1 Эксплуатационные процедуры и обязанности

Цель: Обеспечить уверенность в надлежащем и безопасном функционировании средств обработки информации.

Должны быть установлены обязанности и процедуры в отношении управления и эксплуатации всех средств обработки информации, включая также разработку соответствующих эксплуатационных процедур.

С целью сведения к минимуму риска неправильного использования систем вследствие небрежности или злого умысла, следует, по возможности, реализовать принцип разграничения обязанностей.

Документальное оформление эксплуатационных процедур

Эксплуатационные процедуры следует документально оформлять, соблюдать и делать доступными для всех нуждающихся в них пользователей.

Документально оформленные процедуры должны быть подготовлены для действий системы, связанных со средствами обработки информации и связи, таких как процедуры запуска и завершения работы компьютеров (серверов), процедуры резервирования, текущего обслуживания и ремонта оборудования, обращения с носителями информации, управление работой в машинном зале и работы с почтой, а также процедуры обеспечения безопасности.

Данные процедуры должны содержать детальные инструкции по выполнению каждой работы, включая:

a) обработку и управление информацией;

b) резервирование;

c) требования в отношении графика работ, включая взаимозависимости между системами, время начала самого ранней работы и время завершения самой последней работы;

d) инструкции по обработке ошибок или других исключительных ситуаций, которые могли бы возникнуть в процессе выполнения работы, включая ограничения на использование системных утилит;

e) необходимые контакты на случай неожиданных эксплуатационных или технических проблем;

f) специальные инструкции по управлению выводом данных и обращению с носителями информации, например использование специальной бумаги для печатающих устройств или управление выводом конфиденциальных данных, включая процедуры по безопасной утилизации выходных данных в случае сбоев в работе ;

g) перезапуск системы и соответствующие процедуры восстановления на случай системных сбоев;

h) управление информацией, содержащейся в контрольных записях и системных журналах .

Эксплуатационные процедуры и документально оформленные процедуры действий системы должны рассматриваться как официальные документы, а изменения в них должны санкционироваться руководством. Если технически возможно, менеджмент информационных систем необходимо осуществлять единообразно, используя одни и те же процедуры, инструментальные средства и утилиты.

Управление изменениями

Изменения в конфигурации средств обработки информации и системах должны контролироваться.

Эксплуатируемые системы и прикладное программное обеспечение должны быть предметом строгого контроля управления изменениями.

В частности, необходимо рассмотреть следующие аспекты:

a) определение и регистрацию существенных изменений;

b) планирование и тестирование изменений;

c) оценку возможных последствий, включая последствия для безопасности, таких изменений;

d) формализованную процедуру утверждения предполагаемых изменений;

e) подробное информирование об изменениях всех заинтересованных лиц;

f) процедуры возврата в исходный режим, включая процедуры и обязанности в отношении отмены и последующего восстановления в случае неудачных изменений и непредвиденных обстоятельств.

С целью обеспечения уверенности в надлежащем контроле всех изменений в оборудовании, программном обеспечении или процедурах, должна быть формально определена ответственность и разработаны соответствующие процедуры управления. При внесении изменений вся необходимая информация должна сохраняться в контрольном журнале.

Неадекватный контроль изменений средств и систем обработки информации - распространенная причина системных сбоев и инцидентов безопасности. Изменения эксплуатационной среды, особенно при переходе от стадии разработки к стадии эксплуатации, могут оказывать влияние на надежность прикладных программ.

Изменения эксплуатируемых систем следует осуществлять только в том случае, если на это имеется обоснованная причина, затрагивающая бизнес, например возрастание риска в отношении системы. Обновление систем новейшими версиями эксплуатируемой системы или прикладных программ не всегда отвечает интересам бизнеса, поскольку оно может привнести большее число уязвимостей и большую нестабильность, чем действующая версия. Могут также потребоваться дополнительное обучение, расходы на лицензирование, поддержка, сопровождение и административный надзор, а также аппаратные средства, особенно в течение периода миграции

Разделение обязанностей

Обязанности и области ответственности должны быть разделены для уменьшения возможностей неавторизованной или непреднамеренной модификации активов организации или их нецелевого использования.

Разделение обязанностей -это способ сведения к минимуму риска нецелевого использования систем вследствие ошибочных или злонамеренных действий пользователей. Необходимо предпринять определенные меры предосторожности, чтобы ни один сотрудник не мог осуществлять доступ, модифицировать или использовать активы, не имея авторизации или не будучи обнаруженным. Инициирование события должно быть отделено от его авторизации. При разработке мер и средств контроля и управления следует учитывать опасность сговора.

Небольшие организации могут признавать разделение обязанностей труднодостижимым, однако, данный принцип должен быть применен насколько это возможно. В случаях, когда разделение обязанностей осуществить затруднительно, следует рассматривать использование альтернативных мер и средств контроля и управления, таких как мониторинг деятельности, использование контрольных записей, а также надзор со стороны руководства. В то же время важно, чтобы аудит безопасности оставался независимым.

Разделение средств разработки, тестирования и эксплуатации

Чтобы снизить риски неавторизованного доступа или изменений эксплуатируемой системы, следует обеспечивать разделение средств разработки, тестирования и эксплуатации

Уровень разделения между средами эксплуатации, тестирования и разработки, необходимый для предотвращения проблем эксплуатации, должен быть определен и при этом должны быть реализованы соответствующие меры и средства контроля и управления.

Необходимо рассмотреть следующие вопросы:

a) правила перевода программного обеспечения из статуса разрабатываемого в статус принятого к эксплуатации должны быть определены и документально оформлены;

b) разработка и эксплуатация программного обеспечения должна осуществляться на различных системах или компьютерах в различных доменах или директориях;

c) компиляторы, редакторы и другие инструментальные средства разработки или системные утилиты не должны быть доступны в среде эксплуатации без крайней необходимости;

d) среда системы тестирования должна эмулировать среду эксплуатации настолько точно, насколько это возможно;

e) чтобы уменьшить риск ошибок, пользователи должны применять различные параметры пользователя для эксплуатируемых и тестовых систем, а в экранных меню должны показываться соответствующие идентификационные сообщения;

f) чувствительные данные не должны копироваться в среду системы тестирования

Деятельность, связанная с разработкой и тестированием, может быть причиной серьезных проблем, например нежелательных изменений файлов или системной среды, а также системных сбоев. В этом случае необходимо поддерживать известную и стабильную среду для выполнения комплексного тестирования и предотвращать несанкционированный доступ разработчиков.

Там, где сотрудники, отвечающие за разработку и тестирование, имеют доступ к действующей системе и ее данным, они могут установить неавторизованную и непротестированную программу или изменить рабочие данные. Применительно к ряду систем такая возможность могла бы быть использована для мошенничества или установки непротестированной или вредоносной программы, что может являться причиной серьезных проблем, связанных с эксплуатацией.

Разработчики и специалисты, проводящие тестирование, могут также быть причиной угроз конфиденциальности эксплуатационной информации. Кроме того, если разработка и тестирование производятся в одной компьютерной среде, это может стать причиной непреднамеренных изменений программного обеспечения или информации. Следовательно, разделение средств разработки, тестирования и эксплуатации целесообразно для уменьшения риска случайного изменения или неавторизованного доступа к программному обеспечению и данным бизнеса среды эксплуатации

2. Менеджмент оказания услуг третьей стороной

Цель: Реализовывать и поддерживать соответствующий уровень информационной безопасности и оказания услуг в соответствии с договорами об оказании услуг третьей стороной.

Организация должна проводить проверку реализации договоров, осуществлять мониторинг соответствия условиям договоров и управление изменениями для обеспечения уверенности в том, что оказанные услуги удовлетворяют всем требованиям, согласованным с третьей стороной

Предоставление услуг

Необходимо обеспечивать уверенность в том, что меры и средства контроля и управления безопасности, определение услуг и уровни предоставления услуг, включенные в договор о предоставлении услуг третьей стороной, реализуются, функционируют и поддерживаются третьей стороной.

Предоставление услуг третьей стороной должно включать согласованные меры по обеспечению безопасности, определению услуг и аспекты менеджмента услуг. Что касается договоров аутсорсинга, организация должна планировать необходимые перемещения (информации, средств обработки информации и др., что должно быть перемещено) и обеспечивать уверенность в том, что безопасность поддерживается на протяжении всего периода перемещения.

Организация должна обеспечивать уверенность в том, что третья сторона поддерживает достаточный объем услуг наряду с реализуемыми планами по обеспечению согласованного уровня непрерывности обслуживания, сохраняемого в случае серьезных отказов обслуживания или бедствия.

Мониторинг и анализ услуг третьей стороны

Необходимо регулярно проводить мониторинг и анализ услуг, отчетов и записей, обеспечиваемых третьей стороной, и регулярно проводить аудиты.

Мониторинг и анализ услуг, обеспечиваемых третьей стороной, должны обеспечивать уверенность в том, что условия, касающиеся информационной безопасности, и условия договоров соблюдаются, и что менеджмент инцидентов и проблем информационной безопасности осуществляется должным образом

Между организацией и третьей стороной должна существовать связь для того, чтобы:

a) осуществлять мониторинг уровней предоставления услуг с целью проверки соблюдения условий договоров;

b) анализировать отчеты, о предоставлении услуг, подготовленные третьей стороной, и проводить регулярные рабочие встречи в соответствии с договорами;

c) обеспечивать информацию об инцидентах информационной безопасности и анализ данной информации третьей стороной и организацией в соответствии с условиями договоров и любыми поддерживающими руководствами и процедурами;

d) анализировать контрольные записи третьей стороны и записи событий, связанных с безопасностью, эксплуатационных проблем, отказов, прослеживания недостатков и разрушений, относящихся к предоставляемым услугам;

e) решать все выявленные проблемы и осуществлять их менеджмент.

Ответственность за управление отношениями с третьей стороной следует возлагать на специально назначенного сотрудника или на группу управления услугами. Кроме того, организация должна обеспечивать уверенность в том, что третья сторона берет на себя ответственность за проверку соответствия и исполнения требований договоров. Для мониторинга выполнения требований договора, в частности, требований информационной безопасности, необходимы достаточный технический опыт и ресурсы. Когда в оказании услуг замечены недостатки, следует принимать соответствующие меры.

Организация должна поддерживать достаточный общий контроль и прослеживаемость всех аспектов безопасности чувствительной или критической информации, или средств обработки информации, которые доступны, обрабатываются или управляются третьей стороной. Организация должна обеспечивать уверенность в том, что она поддерживает прослеживаемость деятельности, связанной с безопасностью, например управление изменениями, выявление уязвимостей и сообщение/реагирование на инциденты информационной безопасности с помощью четко определенного процесса, формата и структуры отчетности.

Организация должна быть осведомлена о том, что основная ответственность за информацию, обрабатываемую третьей стороной в рамках договоров аутсорсинга, остается за организацией.

Управление изменениями услуг третьей стороны

Изменения в предоставлении услуг, включая поддержку и улучшение существующих политик, процедур, мер и средств контроля и управления информационной безопасности, должны осуществляться с учетом критичности затрагиваемых систем и процессов бизнеса, а также переоценки рисков.

Процесс управления изменениями услуг третьей стороны, должен учитывать:

a) изменения, проводимые организацией, для реализации:

1) улучшения предлагаемых текущих услуг;

2) разработки каких-либо новых прикладных программ и систем;

3) модификаций или обновлений политик и процедур организации;

4) новых мер и средств контроля и управления для устранения инцидентов информационной безопасности и повышения безопасности;

b) изменения в услугах третьей стороны, для реализации:

1) изменений и улучшений в отношении сетей;

2) использования новых технологий;

3) использования новых продуктов или новейших версий/выпусков;

4) новых инструментальных средств и сред разработки;

5) изменений физического расположения средств обслуживания;

6) смены поставщиков

3 Планирование и приемка систем

Цель: Свести к минимуму риск сбоев в работе систем.

Предварительное планирование и подготовка необходимы для обеспечения адекватной производительности и ресурсов, чтобы получить требуемые эксплуатационные данные системы.

Необходимо составить прогноз в отношении требований и перспективной производительности систем с целью снижения риска их перегрузки.

Эксплуатационные требования для новых систем должны быть определены, документально оформлены и протестированы перед их приемкой и использованием.

Управление производительностью

Использование ресурсов необходимо прогнозировать, исходя из будущих требований к производительности, настраивать и контролировать, чтобы обеспечить уверенность в достижении требуемых эксплуатационных данных системы.

Для каждой новой и продолжающейся деятельности необходимо определять требования к производительности. Следует проводить настройку и контроль систем для обеспечения, где необходимо, уверенности в повышении доступности и эффективности систем. Необходимо применять выявляющие меры и средства контроля и управления, своевременно указывающие на проблемы. Прогнозирование требований к производительности должно учитывать новые требования бизнеса и новые системные требования, а также текущие и прогнозируемые тенденции в отношении возможностей обработки информации организации.

Особое внимание необходимо уделять любым ресурсам, требующим длительного времени на закупку или больших расходов, поэтому руководителям следует осуществлять контроль использования ключевых системных ресурсов. Они должны определять тенденции в использовании, в частности, касающиеся прикладных программ для бизнеса или инструментальных средств информационных систем управления.

Руководителям следует использовать эту информацию с целью выявления потенциально узких мест и зависимости от ключевого персонала, который мог бы представлять угрозу безопасности систем или сервисов, и планирования соответствующего действия.

Приемка систем

Должны быть определены критерии приемки для новых информационных систем, обновлений и новых версий, кроме того, необходимо тестировать системы в течение их разработки и перед их приемкой.

Руководители должны обеспечить уверенность в том, что требования и критерии для принятия новых систем четко определены, согласованы, документально оформлены и протестированы. Новые информационные системы, обновления и новые версии должны вводиться в эксплуатацию только после прохождения официальной приемки.

До официальной приемки необходимо рассмотреть следующие аспекты:

a) требования к мощности и производительности компьютера;

b) процедуры восстановления после сбоев и перезапуска, и планы действий в чрезвычайных ситуациях;

c) подготовка и тестирование типовых операционных процедур на соответствие установленным стандартам;

d) наличие согласованного набора меры и средства контроля и управления безопасности;

e) эффективные ручные процедуры;

f) мероприятия по обеспечению непрерывности бизнеса ;

g) документальное подтверждение того, что внедрение новой системы не будет неблагоприятно влиять на существующие системы, особенно, во время максимальных нагрузок, например в конце месяца;

h) документальное подтверждение того, что было учтено влияние, оказываемое новой системой, на общую безопасность организации;

i) тренинг в отношении эксплуатации и использования новых систем;

j) простота использования, поскольку это влияет на производительность работы пользователя и позволяет избегать ошибок оператора.

В отношении новых крупных разработок, службы поддержки и пользователи должны привлекаться для консультации на всех стадиях процесса разработки с целью эффективного проектирования системы. Соответствующие тесты должны проводиться для подтверждения того, что все критерии приемки удовлетворены полностью.

Приемка может включать формальный процесс сертификации и аккредитации для подтверждения того, что требования к безопасности были учтены должным образом.

4 Защита от вредоносной и мобильной программы

Цель: Защита целостности программного обеспечения и информации.

Необходимо принимать меры предосторожности для предотвращения и обнаружения вредоносной программы и неавторизованной мобильной программы.

Программное обеспечение и средства обработки информации уязвимы по отношению к внедрению вредоносной программы, такой как компьютерные вирусы, сетевые "черви", "троянские кони" и логические бомбы. Пользователи должны быть осведомлены об опасности, связанной с вредоносной программой. Руководители должны, при необходимости, обеспечить внедрение мер и средств контроля и управления с целью предотвращения, обнаружения и удаления вредоносной программы и контролирования мобильной программы.

Меры и средства контроля и управления против вредоносной программы

Необходимо внедрить меры и средства контроля и управления, связанные с обнаружением, предотвращением и восстановлением, с целью защиты от вредоносной программы, а также процедуры, обеспечивающие соответствующую осведомленность пользователей.

Защита от вредоносной программы должна основываться: на обнаружении вредоносной программы и восстановлении программного обеспечения; на понимании требований безопасности; на мерах и средствах контроля и управления соответствующего доступа к системе и менеджмента изменений.

Необходимо рассмотреть следующие рекомендации:

a) создать официальную политику, устанавливающую запрет на использование неавторизованного программного обеспечения ;

b) создать официальную политику защиты от рисков, связанных с получением файлов и программного обеспечения, либо из внешних сетей, либо через другие передающие среды, показывающую, какие защитные меры следует принять;

c) проводить регулярный анализ программного обеспечения и содержания данных систем, поддерживающих критические процессы бизнеса; необходима формальная процедура расследования причин наличия любых неавторизованных или измененных файлов

d) осуществлять в качестве превентивной меры или обычным порядком инсталляцию и регулярное обновление программного обеспечения по обнаружению вредоносной программы и восстановлению для сканирования компьютеров и носителей информации; проводимые проверки должны включать:

1) проверку на наличие вредоносной программы любых файлов на электронных или оптических носителях и файлов, полученных из сетей перед их использованием;

2) проверку любых вложений электронной почты и скачиваемой информации до их использования на наличие вредоносной программы; эта проверка должна выполняться в разных точках, например на серверах электронной почты, настольных компьютерах или при входе в сеть организации;

3) проверку web-страниц на наличие вредоносной программы;

e) определять управленческие процедуры и обязанности, связанные с защитой от вредоносной программы в системах, тренинг их использования, оповещение и восстановление после атак вредоносной программы;

f) подготовить соответствующие планы по обеспечению непрерывности бизнеса в части восстановления после атак вредоносной программы, включая все необходимые мероприятия по резервированию и восстановлению данных и программного обеспечения;

g) реализовать процедуры регулярного сбора информации, например подписываясь на список почтовой рассылки и (или) проверяя web-сайты, дающие информацию о новой вредоносной программе;

h) реализовать процедуры проверки информации, касающейся вредоносной программы, и обеспечить точность и информативность предупредительных сообщений; соответствующие руководители должны обеспечить уверенность в том, что компетентные источники, например информация из известных журналов, заслуживающих доверия Интернет-сайтов или от поставщиков антивирусного программного обеспечения используется для определения различий между ложной и реальной вредоносной программой; все пользователи должны быть осведомлены о проблеме ложных вирусов и действиях при их получении.

Использование двух или более программных продуктов, обеспечивающих защиту от вредоносной программы в среде обработки информации, от разных поставщиков может повысить эффективность данной защиты.

Для защиты от вредоносной программы может устанавливаться программное обеспечение, позволяющее проводить автоматические обновления определенных файлов и сканирование машин для подтверждения актуальности защиты. Кроме того, такое программное обеспечение может быть установлено на каждом рабочем столе для выполнения автоматических проверок.

Следует заботиться о защите от внедрения вредоносной программы во время процедур по техническому обслуживанию и процедур, связанных с критическими ситуациями, когда можно обойти обычные меры и средства контроля и управления, применяемые для защиты от вредоносной программы.

*Меры и средства контроля и управления при использовании мобильной программ*ы

Там, где разрешено использование мобильной программы, конфигурация должна обеспечивать уверенность в том, что разрешенная мобильная программа функционирует в соответствии с ясно сформулированной политикой безопасности, а исполнение неразрешенной мобильной программы будет запрещено.

Для предотвращения выполнения мобильной программой неразрешенных действий необходимо принимать следующие меры:

a) обеспечивать выполнение мобильной программы в логически изолированной среде;

b) блокировать любое несанкционированное использование мобильной программы;

c) блокировать прием мобильной программы;

d) активизировать технические меры, доступные в отношении определенной системы, чтобы обеспечить уверенность в управляемости мобильной программы;

e) контролировать ресурсы, доступные мобильной программе;

c) блокировать прием мобильной программы;

d) активизировать технические меры, доступные в отношении определенной системы, чтобы обеспечить уверенность в управляемости мобильной программы;

e) контролировать ресурсы, доступные мобильной программе;

f) применять криптографические меры и средства контроля и управления для однозначной аутентификации мобильной программы.

Мобильная программа представляет собой программный код, который переходит с одного компьютера на другой, а затем исполняется автоматически, и выполняет определенную функцию без какого-либо взаимодействия с пользователем или при минимальном взаимодействии с ним. Мобильная программа связана с рядом услуг вспомогательного программного обеспечения.

В дополнение к обеспечению уверенности в том, что мобильная программа не содержит вредоносного кода, важно контролировать мобильную программу с целью предотвращения неавторизованного использования или разрушения системных, сетевых или прикладных ресурсов и других нарушений информационной безопасности.

5 Резервирование

Цель: Поддерживать целостность и доступность информации и средств обработки информации.

Должны быть созданы типовые процедуры по реализации установленной политики и стратегии резервирования в отношении снятия резервных копий данных и обеспечения их своевременного восстановления.

Резервирование информации

Резервное копирование информации и программного обеспечения должно выполняться и тестироваться на регулярной основе в соответствии с установленной политикой резервирования.

Следует обеспечить адекватные средства резервирования для обеспечения уверенности в том, что вся важная информация и программное обеспечение могут быть восстановлены после бедствия или сбоя оборудования.

В отношении резервирования информации необходимо рассматривать следующие вопросы:

a) необходимо определить надлежащий уровень резервной информации;

b) необходимо обеспечивать точные и полные записи резервных копий и документально оформленные процедуры восстановления;

c) объем (т.е. полное или выборочное резервирование) и частота резервирования должны отражать требования бизнеса организации, требования к безопасности затрагиваемой информации и критичность информации для непрерывной работы организации;

d) резервные копии должны храниться в удаленном месте, на надежном расстоянии, достаточном, чтобы избежать любого повреждения вследствие аварийной ситуации в основном здании;

e) в отношении резервной информации должен быть обеспечен соответствующий уровень физической защиты и защиты от воздействий окружающей среды, в соответствии со стандартами, применяемыми в основном здании; меры и средства контроля и управления, применяемые к носителям информации в основном здании, должны также применяться и на резервной площадке;

f) носители резервной информации должны регулярно тестироваться для обеспечения уверенности в том, что в случае чрезвычайных ситуаций они могут быть использованы;

g) процедуры восстановления следует регулярно проверять и тестировать для обеспечения уверенности в их эффективности, а также в том, что для выполнения этих процедур потребуется не больше времени, чем это определено;

h) в ситуациях, когда конфиденциальность играет важную роль, резервные копии необходимо защищать посредством шифрования

Мероприятия по резервированию, применяемые в отношении отдельных систем, должны регулярно тестироваться для обеспечения уверенности в том, что они удовлетворяют требованиям, содержащимся в планах непрерывности бизнеса . Применительно к критическим системам, мероприятия по резервированию должны охватывать информацию, прикладные программы и данные всех систем, необходимые для восстановления целой системы в случае бедствия.

Следует определить сроки хранения важной информации бизнеса, а также любое требование к архивным копиям, подлежащим длительному хранению .

Для упрощения процесса резервирования и восстановления мероприятия по резервированию могут быть автоматизированы. Такие решения по автоматизации должны в достаточной мере и регулярно тестироваться, прежде чем они будут реализованы

6 Менеджмент безопасности сети

Цель: Обеспечить уверенность в защите информации в сетях и защите поддерживающей инфраструктуры

Менеджмент безопасности сетей, которые могут проходить за пределами организации, требует пристального внимания к потокам данных, правовым последствиям, мониторингу и защите.

Дополнительные меры и средства контроля и управления могут также потребоваться для защиты чувствительной информации, передаваемой по общедоступным сетям.

Меры и средства контроля и управления сетями

Сети должны адекватно управляться и контролироваться, чтобы быть защищенными от угроз и обеспечить безопасность систем и прикладных программ, использующих сеть, включая информацию во время ее передачи.

Руководители, отвечающие за поддержку сетевых ресурсов, должны внедрять меры и средства контроля и управления для обеспечения уверенности в безопасности информации в сетях и защиты подключенных сервисов от неавторизованного доступа. В частности, необходимо рассмотреть следующие вопросы:

a) следует разделить, где это необходимо, ответственность за поддержку сетевых ресурсов и за поддержку компьютерных операций;

b) следует определить обязанности и процедуры для управления удаленным оборудованием, включая оборудование, установленное у конечных пользователей;

c) специальные меры и средства контроля и управления следует внедрить для обеспечения конфиденциальности и целостности данных, передаваемых по общедоступным сетям, или по беспроводным сетям, а также для защиты подключенных систем и прикладных программ (см. 11.4 и 12.3); специальные меры и средства контроля и управления могут потребоваться для поддержки доступности сетевых сервисов и рабочих станций;

d) соответствующая регистрация и мониторинг должны применяться с целью обеспечения возможности регистрации действий, имеющих значение для безопасности;

e) действия руководства должны быть тщательно согласованы как для оптимизации получаемых организацией услуг, так и для обеспечения уверенности в том, что меры и средства контроля и управления единообразно применимы ко всей инфраструктуре обработки информации.

Безопасность сетевых услуг

Средства обеспечения безопасности, уровни услуг и требования в отношении менеджмента всех сетевых услуг должны быть определены и включены в любой договор по сетевым услугам, вне зависимости оттого, будут ли они обеспечиваться силами организации или в рамках договоров аутсорсинга.

Способность провайдера сетевых услуг безопасно осуществлять менеджмент установленных услуг следует определять и подвергать регулярному мониторингу, а право проведения аудита должно быть согласовано.

Должны быть определены меры безопасности, необходимые для конкретных услуг, например средства обеспечения безопасности, уровни услуг и требования в отношении менеджмента. Организация должна обеспечивать уверенность в том, что провайдеры сетевых услуг реализуют эти меры.

Сетевые услуги включают в себя обеспечение соединений, услуг частных сетей и сетей с дополнительными функциями, а также решений, касающихся управления безопасностью сети, например межсетевые экраны и системы обнаружения вторжения. Такие услуги могут варьироваться от простых решений, касающихся неуправляемой пропускной способности, до сложных решений с обеспечением дополнительных услуг.

Средствами обеспечения безопасности сетевых услуг могут быть:

a) средства, применяемые для обеспечения безопасности сетевых услуг, например аутентификация, шифрование, и меры и средства контроля и управления сетевыми соединениями;

b) соблюдение технических параметров, требуемых для безопасного подключения сетевых услуг в соответствии с правилами безопасности сетевых соединений;

c) процедуры использования сетевой услуги, применяемые для ограничения доступа к сетевым услугам или прикладным программам, где это необходимо.

7 Обращение с носителями информации

Цель: Предотвратить неавторизованное раскрытие, модификацию, выбытие или уничтожение активов и прерывание деятельности бизнеса.

Использование носителей информации должно контролироваться, необходимо также обеспечить их физическую безопасность.

Должны быть определены соответствующие процедуры в отношении защиты документов, компьютерных носителей информации (например лент, дисков), данных ввода/вывода и системной документации от неавторизованного раскрытия, модификации, выноса и уничтожения.

Менеджмент сменных носителей информации

Должны существовать процедуры в отношении менеджмента сменных носителей информации

Необходимо рассмотреть следующие рекомендации в отношении менеджмента сменных носителей информации:

a) если не предполагается повторно использовать содержание носителей информации, которые должны быть перемещены за пределы организации, то информацию необходимо сделать неизвлекаемой;

b) где необходимо и практично, должно требоваться разрешение на вынос носителей информации из организации и запись о таком перемещении следует хранить как контрольную запись для аудита;

c) все носители информации должны храниться в надежной, безопасной среде, в соответствии со спецификациями изготовителей;

d) информацию, хранимую на носителях, востребованную дольше, чем жизненный цикл носителя (в соответствии со спецификациями изготовителей), следует хранить также и в другом месте, во избежание потери информации вследствие износа носителей;

e) для уменьшения возможности потери данных должна быть предусмотрена регистрация сменных носителей информации;

f) сменные дисковые накопители разрешается использовать только в случае, обусловленном потребностями бизнеса.

Все процедуры и уровни авторизации должны быть четко зафиксированы документально.

К сменным носителям информации относятся ленты, диски, диски флэш-памяти, сменные жесткие диски, CD, DVD и печатные носители информации.

Утилизация носителей информации

Носители информации, когда в них больше нет необходимости, следует надежно и безопасно утилизировать, используя формальные процедуры.

Формальные процедуры для безопасной утилизации носителей информации должны снижать риск утечки чувствительной информации неавторизованным лицам. Процедуры для безопасной утилизации носителей, содержащих чувствительную информацию, должны соответствовать чувствительности той информации. Необходимо рассмотреть следующие вопросы:

a) носители, содержащие чувствительную информацию, должны храниться и утилизироваться надежно и безопасно, например посредством сжигания или измельчения; если носители планируется использовать в пределах организации для других прикладных программ, информация на них должна быть уничтожена;

b) должны существовать процедуры по выявлению носителей информации, для которых может потребоваться безопасная утилизация;

c) может оказаться проще принимать меры по сбору и безопасной утилизации в отношении всех носителей информации, чем пытаться выделить носители с чувствительной информацией;

d) многие организации предлагают услуги по сбору и утилизации бумаги, оборудования и носителей информации; следует тщательно выбирать подходящего подрядчика с учетом имеющегося у него опыта и применяемых мер и средств контроля и управления;

e) где возможно, утилизацию носителей, содержащих чувствительную информацию, следует фиксировать как контрольную запись для аудита.

При накоплении носителей информации, подлежащих утилизации, следует принимать во внимание "эффект накопления", т е. большое количество нечувствительной информации делает ее чувствительной.

Чувствительная информация может быть раскрыта при небрежной утилизации носителей.

Процедуры обработки информации

С целью обеспечения защиты информации от неавторизованного раскрытия или неправильного использования необходимо определить процедуры обработки и хранения информации.

Должны быть разработаны процедуры по ручной обработке информации, обработке информации с использованием компьютеров, хранению и передаче информации в соответствии с ее классификацией (см. 7.2). Необходимо рассмотреть следующие вопросы:

a) обработку и маркировку всех носителей информации в соответствии с ее указанным уровнем классификации;

b) ограничение доступа с целью предотвращения доступа неавторизованного персонала;

c) обеспечение формальной регистрации авторизованных получателей данных;

d) обеспечение уверенности в том, что процесс ввода данных и обработки завершаются должным образом и что выполняется проверка выходных данных;

e) защиту информации, находящейся в буфере данных и ожидающей вывода, соответствующую степени чувствительности этой информации;

f) хранение носителей информации в соответствии со спецификациями изготовителей;

g) сведение распространения данных к минимуму;

h) четкая маркировка всех копий данных, предназначенных вниманию авторизованного получателя;

i) пересмотр списков рассылки и списков авторизованных получателей через регулярные интервалы времени.

Эти процедуры применяются к информации в документах, вычислительным системам, сетям, переносным компьютерам, мобильным средствам связи, почте, речевой почте, речевой связи вообще, мультимедийным устройствам, почтовым услугам/устройствам, к использованию факсов и любых других чувствительных объектов, например бланков чеков и счетов.

Безопасность системной документации

Системная документация должна быть защищена от неавторизованного доступа.

Для защиты системной документации необходимо учитывать следующие вопросы:

a) системную документацию надлежит хранить безопасным образом;

b) список лиц, имеющих доступ к системной документации, необходимо свести к минимуму; доступ должен быть авторизован владельцем прикладной программы;

c) системную документацию, полученную или поддерживаемую через общедоступную сеть, следует защищать надлежащим образом.

Системная документация может содержать разнообразную чувствительную информацию, например описание процессов работы прикладных программ, процедур, структур данных, процессов авторизации.

8. Обмен информацией

Цель: Поддерживать безопасность информации и программного обеспечения, обмениваемых в пределах организации и с любым внешним объектом.

Обмен информацией и программным обеспечением между организациями должен основываться на формальной политике обмена, осуществляться в соответствии с соглашениями по обмену и соответствовать действующему законодательству

Необходимо определить процедуры и стандарты по защите информации и ее физических носителей при передаче.

Политики и процедуры обмена информацией

Должны существовать формальные политики, процедуры и меры и средства контроля и управления в отношении обмена информацией с целью защиты такого обмена, когда используются все типы средств связи.

Процедуры, меры и средства контроля и управления, которые необходимо соблюдать при использовании электронных средств связи для обмена информацией, должны учитывать следующее:

a) процедуры, предназначенные для защиты обмениваемой информации от перехвата, копирования, модификации, ложной маршрутизации и разрушения;

b) процедуры обнаружения вредоносной программы, которая может передаваться при использовании электронных средств связи, и процедуры защиты от неё ;

c) процедуры защиты передаваемой чувствительной электронной информации, имеющей форму приложения;

d) политику или рекомендации, определяющие приемлемое использование электронных средств связи

e) процедуры использования беспроводной связи, учитывая сопряженные с ней определенные риски;

f) обязательство сотрудника, подрядчика и любого другого представителя не компрометировать организацию, например посредством клеветы, антисоциальных действий, выдачи себя за другое лицо, распространения "писем счастья", использования "тайных рычагов" и т д.;

g) использование криптографических методов, например для защиты конфиденциальности, целостности и аутентичности информации ;

h) рекомендации по сохранению и утилизации всей деловой корреспонденции, включая сообщения, в соответствии с действующими национальными и местными законодательными и нормативными актами;

i) напоминание сотрудникам о том, что нельзя оставлять чувствительную или критическую информацию на печатающих устройствах, например копировальных устройствах, принтерах и факсах, поскольку неавторизованный персонал может осуществлять к ним доступ;

j) меры и средства контроля и управления и ограничения, связанные с пересылкой средств связи, например автоматическая пересылка электронной почты на внешние почтовые адреса;

к) напоминание сотрудникам о необходимости соблюдения мер предосторожности, например не следует разглашать чувствительную информацию во избежание ее подслушивания или перехвата при телефонных звонках:

1) лицами, находящимися в непосредственной близости, особенно при использовании мобильных телефонов;

2) при прослушивании телефонных переговоров и других формах подслушивания путем физического доступа к трубке или телефонной линии, или при использовании сканирующих приемников;

3) посторонними лицами на стороне адресата;

l) напоминание сотрудникам о том, что нельзя оставлять сообщения, содержащие чувствительную информацию, на автоответчиках, поскольку они могут быть прослушаны неавторизованными лицами, храниться в общественных системах или неверно помещены на хранение вследствие ошибки соединения;

m) напоминание сотрудникам о проблемах, связанных с использованием факсов, а именно:

1) неавторизованный доступ к встроенной памяти для поиска сообщений;

2) преднамеренное или случайное перепрограммирование аппаратов с целью передачи сообщений по определенным номерам;

3) отсылка документов и сообщений по неправильному номеру вследствие ошибки в наборе, либо из-за использования неправильно сохраненного номера;

n) напоминание сотрудникам о том, что не следует регистрировать демографические данные, например адрес электронной почты или другую личную информацию, в каком-либо программном обеспечении, во избежание ее сбора для неавторизованного использования;

o) напоминание сотрудникам о том, что современные факсимильные и фотокопирующие устройства оснащены страничной кэш-памятью, и "запоминают" страницы в случае проблем с бумагой или передачей, которые будут напечатаны после устранения неисправности.

Кроме того, необходимо напоминать сотрудникам о том, что не следует вести конфиденциальные беседы в общественных местах или открытых офисах, а также в переговорных комнатах, стены которых не защищены звукоизоляцией.

Средства обмена информацией должны соответствовать любым действующим законодательным требованиям

Обмен информацией может осуществляться при использовании различных типов коммуникационных средств, включая электронную почту, факсимильные, аудио- и видео- средства.

Обмен программным обеспечением может осуществляться при использовании различных типов носителей информации, включая "скачивание" из Интернета и приобретение у поставщиков, продающих готовые продукты

Следует учитывать подразумеваемые положения бизнеса, законодательства и безопасности, связанные с электронным обменом данными, электронной торговлей и электронными коммуникациями, а также и с требованиями к мерам и средствам контроля и управления.

Информация может быть скомпрометирована из-за недостатка осведомленности сотрудников в отношении политики или процедур по использованию средств обмена информацией, например вследствие подслушивания при переговорах по мобильному телефону в общественном месте, отправления сообщения электронной почты по неправильному адресу, прослушивания автоответчиков, неавторизованного доступа к системам голосовой почты или случайной отсылки факсимильных сообщений неправильному адресату.

Операции бизнеса могут быть прерваны и информация может быть скомпрометирована в случае отказа, перегрузки или прерывания в работе средств связи. Информация может быть скомпрометирована вследствие доступа неавторизованных пользователей.

Соглашения по обмену информацией

Необходимо заключать соглашения по обмену информацией и программным обеспечением между организацией и сторонними организациями.

В соглашениях по обмену следует учитывать следующие условия безопасности:

a) обязанности руководства в отношении контроля и уведомления о передаче, отправке и получении;

b) процедуры уведомления отправителя, а также процедуры передачи, отправки и получения;

c) процедуры обеспечения прослеживаемости и неотказуемости;

d) минимальные требования технических стандартов по формированию и передаче пакетов данных;

e) соглашения в отношении передачи на хранение исходных пакетов данных;

f) стандарты в отношении курьерской службы;

g) ответственность и обязательства в случае инцидентов информационной безопасности, например в случае потери данных;

h) использование согласованной системы маркировки для критической или чувствительной информации, обеспечивающей уверенность в том, что значение этой маркировки будет сразу же понято и что информация будет соответственно защищена;

i) право собственности и обязанности по защите данных, соблюдение авторских прав, соответствие лицензии на программное обеспечение и аналогичные требования ;

j) технические стандарты в отношении записи и считывания информации и программного обеспечения;

к) любые специальные меры и средства контроля и управления, которые могут потребоваться для защиты чувствительных элементов, например криптографических ключей.

Необходимо создавать и поддерживать политики, процедуры и стандарты в отношении защиты информации и физических носителей информации при их пересылке , а в соглашении по обмену следует делать на них ссылку.

Содержание любого соглашения в части безопасности должно отражать чувствительность затрагиваемой информации бизнеса.

Соглашения могут существовать в электронном или физическом виде и могут иметь форму официальных договоров или условий найма. В отношении чувствительной информации, определенные механизмы, используемые для обмена такой информацией, должны быть единообразны для всех организаций и типов соглашений.

Физические носители информации при транспортировке

Носители информации должны быть защищены от неавторизованного доступа, неправильного использования или повреждения во время их транспортировки за пределами организации.

Для защиты носителей информации, передаваемых между различными пунктами назначения, необходимо учитывать следующие рекомендации:

a) необходимо пользоваться услугами надежных перевозчиков или курьеров;

b) список авторизованных курьеров необходимо согласовывать с руководством;

c) необходимо разработать процедуры для проверки идентификации курьеров;

d) упаковка должна быть достаточно прочной для защиты от любого физического повреждения, которое, вероятно, может иметь место при транспортировке, и соответствовать любым требованиям изготовителей (например программного обеспечения), необходимо обеспечивать защиту от воздействия любых факторов окружающей среды, которые могут снизить эффективность восстановления, таких как тепловой эффект, влажность или электромагнитные поля;

е) меры и средства контроля и управления следует применять, где это необходимо, для защиты чувствительной информации от неавторизованного раскрытия или модификации, например:

1) использование запертых контейнеров;

2) личная доставка;

3) использование упаковки, которую нельзя нарушить незаметно (на которой видна любая попытка вскрытия);

4) в исключительных случаях, разбивка отправления на несколько частей, пересылаемых раз-личными маршрутами.

Информация может быть уязвимой вследствие неавторизованного доступа, неправильного использования или искажения во время физической транспортировки, например при пересылке носителей информации по почте или через курьера.

Электронный обмен сообщениями

Необходимо должным образом защищать информацию, включаемую в электронный обмен сообщениями.

В отношении электронного обмена сообщениями, необходимо учитывать следующие вопросы, связанные с обеспечением безопасности:

a) защита сообщений от неавторизованного доступа, модификации или отказа в обслуживании;

b) обеспечение правильной адресации и передачи сообщения;

c) общая надежность и доступность услуг;

d) законодательные вопросы, например требования в отношении использования электронных подписей;

e) получение одобрения до использования внешних общедоступных услуг, таких как мгновенный обмен сообщениями или разделение файлов;

f) строгие уровни аутентификации управления доступом со стороны общедоступных сетей.

Электронный обмен сообщениями, например электронная почта, обмен данными в электронном виде и мгновенный обмен сообщениями, играет все более важную роль в коммуникациях бизнеса. Риски, связанные с электронным обменом сообщениями, отличаются от рисков, присущих передаче сообщений на бумаге.

Информационные системы бизнеса

Необходимо разработать и внедрить политики и процедуры защиты информации, связанной с взаимодействием информационных систем бизнеса.

Необходимо учитывать последствия от взаимодействия информационных систем для безопасности и бизнеса в целом, такие как:

a) известная уязвимость, присущая административным системам и системам учета и отчетности, где информация разделяется между различными частями организации;

b) уязвимость информации в системах связи бизнеса, например записи телефонных разговоров или переговоров по конференц-связи, конфиденциальность звонков, хранение факсов, вскрытие и рассылка электронных сообщений;

c) политика и соответствующие меры и средства контроля и управления для менеджмента совместного использования информации;

d) запрет на использование чувствительной информации бизнеса и не подлежащих оглашению документов, если данные системы не обеспечивают соответствующий уровень защиты ;

e) ограничение доступа к данным личных ежедневников отдельных сотрудников, например работающих над чувствительными проектами;

f) определение категорий тех сотрудников, подрядчиков или деловых партнеров, которым разрешено использовать систему, и точек, с которых может осуществляться доступ к ней ;

g) ограничение отдельных возможностей системы для определенных категорий пользователей;

h) определение статуса пользователей, например сотрудников организации или подрядчиков, в отдельных директориях, для удобства других пользователей;

i) сохранение и резервное копирование информации, содержащейся в системе;

j) условия перехода на аварийный режим работы и перечень соответствующих мероприятий .

Офисные информационные системы обеспечивают возможность быстрого распространения и совместного использования информации бизнеса и представляют собой комбинацию документов, компьютеров, переносных компьютеров, мобильных средств связи, почты, голосовой почты, речевой связи, мультимедийных систем, услуг доставки почтовых отправлений и факсов.

9. Услуги электронной торговли

Цель: Обеспечить уверенность в безопасности услуг электронной торговли и их безопасном использовании.

Следует учитывать последствия для безопасности, связанные с использованием услуг электронной торговли, включая транзакции в режиме онлайн, и необходимость мер и средств контроля и управления. Необходимо рассматривать также целостность и доступность информации, публикуемой электронным образом при использовании общедоступных сетей.

Информация, используемая в электронной торговле, проходящая по общедоступным сетям, должна быть защищена от мошенничества, оспаривания договоров, а также неавторизованного раскрытия и модификации.

В отношении электронной торговли необходимо рассмотреть следующие вопросы в области безопасности:

a) степень защищенности каждой стороны при идентификации друг друга, например посредством аутентификации;

b) процессы авторизации в отношении того, кто может устанавливать цены, выпускать или подписывать ключевые коммерческие документы;

c) обеспечение уверенности в том, что торговые партнеры полностью проинформированы о своих авторизациях;

d) определение и удовлетворение требований в отношении конфиденциальности, целостности, подтверждения отправки и получения ключевых документов, а также невозможности отказа от совершенных сделок, например связанных с процессами заключения контрактов и проведения тендеров;

e) уровень доверия, вкладываемого в достоверность рекламируемых прайс-листов;

f) конфиденциальность любых чувствительных данных или информации;

g) конфиденциальность и целостность любой информации о сделках, связанных с заказом, условиях оплаты и адресах поставки, а также подтверждения при его получении;

h) степень контроля, достаточная для проверки информации об оплате, представленной клиентом;

i) выбор формы оплаты, наиболее защищенной от мошенничества;

j) уровень защиты, необходимый для обеспечения конфиденциальности и целостности информации о заказах;

к) предотвращение потери или дублирования информации о сделках;

l) ответственность за любые мошеннические сделки;

m) страховые требования.

Многие из вышеупомянутых проблем могут быть решены с использованием криптографических мер и средств контроля и управления), при этом необходимо обеспечить соответствие требованиям законодательства ,

Соглашения в области электронной торговли между партнерами следует подкреплять документально оформленными договорами, которые устанавливают согласованные между сторонами условия заключения сделок, включая подробную процедуру авторизации. Могут потребоваться также дополнительные соглашения с поставщиками сетевых и информационных услуг.

Общественные системы торговли должны обнародовать условия заключения сделок с клиентами.

Необходимо обеспечить устойчивость к компьютерным атакам на основной(ые) сервер(ы) электронной торговли, а также рассмотреть последствия для безопасности всех сетевых взаимосвязей, необходимых для реализации решений электронной торговли .

Электронная торговля уязвима по отношению к сетевым угрозам, которые могут привести к краже, оспариванию договоров, а также к раскрытию или модификации информации.

Для снижения рисков электронная торговля может воспользоваться заслуживающими доверия методами аутентификации, например использующими криптографию с открытым ключом и цифровые подписи. Там, где необходимо, могут использоваться услуги третьей доверенной стороны.

Транзакции в режиме онлайн

Информацию, используемую в онлайн транзакциях, следует защищать для предотвращения неполной передачи, неправильной маршрутизации, неавторизованного изменения сообщений, неавторизованного раскрытия, неавторизованного дублирования или воспроизведения сообщений.

Вопросы безопасности транзакций в режиме онлайн должны включать:

a) использование электронных подписей каждой из сторон, участвующих в транзакции;

b) все аспекты транзакции, т е. обеспечение уверенности в том, что:

1) пользовательские мандаты всех сторон действительны и проверены;

2) транзакция остается конфиденциальной;

3) приватность всех участвующих сторон сохраняется;

c) канал связи между всеми участвующими сторонами зашифрован;

d) протоколы, используемые для установления связи между всеми участвующим сторонами, защищены;

e) обеспечение уверенности в том, что хранение деталей транзакции обеспечивается за пределами любой общедоступной среды, например на платформе хранения, имеющейся в Интернете организации, а не в среде хранения, доступной непосредственно из Интернета;

f) там, где используются услуги доверенного органа (например в целях создания и поддержки цифровых подписей и (или) цифровых сертификатов), безопасность обеспечивается как интегрированная и неотъемлемая часть на протяжении всего сквозного процесса менеджмента подписей/сертификатов.

Объем применяемых мер и средств контроля и управления необходимо соизмерять с уровнем риска, связанным с каждой формой онлайн транзакции. Может возникнуть необходимость соблюдения законов, правил и нормативов в рамках той юрисдикции, в которой транзакция формируется, обрабатывается, завершается и (или) хранится.

Существует много транзакций, которые могут быть выполнены онлайн способом, например контрактные, финансовые и другие.

Общедоступная информация

Целостность информации, которая доступна в общедоступной системе, следует защищать для предотвращения неавторизованной модификации.

Программное обеспечение, данные и другая информация, для которых требуется высокий уровень целостности и которые доступны в общедоступной системе, необходимо защищать с помощью соответствующих механизмов, например цифровых подписей. Общедоступная система должна быть протестирована на предмет недостатков и отказов прежде, чем информация станет доступной.

Должен применяться формальный процесс утверждения прежде, чем информация станет общедоступной. Кроме того, все материалы, представленные в систему извне, должны быть проверены и утверждены.

Системы электронной публикации, особенно те, которые предоставляют возможности обратной связи и непосредственного ввода информации, должны находиться под тщательным контролем, с тем чтобы:

a) информация была получена в соответствии со всеми требованиями законодательства в отношении защиты данных;

b) информация, введенная в систему электронной публикации, обрабатывалась полностью, точно и своевременно;

c) чувствительная информация должна быть защищена в процессе ее сбора, обработки и хранения;

d) доступ к системе электронной публикации исключал возможность непреднамеренного доступа к сетям, с которыми она связана.

Информацию, размещенную в общедоступной системе, например на доступном через Интернет Web-сервере, возможно, будет необходимо привести в соответствие с законами, правилами и нормами той юрисдикции, в которой находится система, где осуществляется торговля или где проживает(ют) владелец(льцы). Неавторизованная модификация опубликованной электронным способом информации может нанести вред репутации организации, разместившей эту информацию.

10 Мониторинг

Цель: Обнаружение неавторизованных действий, связанных с обработкой информации.

Системы должны контролироваться и события информационной безопасности должны быть зарегистрированы. Для обеспечения уверенности в том, что проблемы информационной системы выявляются, следует вести журналы эксплуатации и регистрировать неисправности

Организация должна выполнять все действующие правовые требования, применимые к ее деятельности, связанной с мониторингом и регистрацией.

Мониторинг систем следует проводить с целью проверки эффективности применяемых мер и средств контроля и управления, а также подтверждения следования модели политики доступа

Контрольная регистрация

Необходимо вести и хранить в течение согласованного периода времени контрольные журналы, регистрирующие действия пользователей, нештатные ситуации и события информационной безопасности, чтобы помочь в будущих расследованиях и проведении контроля управления доступом.

Контрольные журналы должны включать, при необходимости:

a) идентификаторы пользователей;

b) даты, время и детали ключевых событий, например начало сеанса и завершение сеанса;

c) идентичность и местоположение терминала, если это возможно;

d) регистрацию успешных и отклоненных попыток доступа к системе;

e) регистрацию успешных и отклоненных попыток доступа к данным или другим ресурсам;

f) изменения конфигурации системы;

g) использование привилегий;

h) использование системных утилит и прикладных программ;

i) файлы, к которым был осуществлен доступ и вид доступа;

j) сетевые адреса и протоколы;

к) сигналы тревоги, подаваемые системой управления доступом;

l) активация и деактивация систем защиты, например антивирусных систем и систем обнаружения вторжения.

Контрольные журналы могут содержать данные о вторжениях и конфиденциальные личные данные. Необходимо принимать соответствующие меры для защиты приватности. Где возможно, системным администраторам следует запрещать стирать или деактивировать журналы регистрации их собственных действий.

Использование системы мониторинга

Необходимо создать процедуры для проведения мониторинга использования средств обработки информации и регулярно анализировать результаты деятельности, связанной с мониторингом.

Уровень мониторинга, необходимый для отдельных средств, следует определять с помощью оценки риска. Организация должна выполнять все действующие законодательные требования, применимые к ее деятельности, связанные с мониторингом.

Необходимо рассмотреть следующие аспекты:

a) авторизованный доступ, включая детали, такие как:

1) идентификаторы пользователей;

2) дату и время основных событий;

3) типы событий;

4) файлы, к которым был осуществлен доступ;

5) используемые программы/утилиты;

b) все привилегированные действия, такие как:

1) использование привилегированных учетных записей, например супервизора, привилегированного пользователя, администратора;

2) запуск и остановка системы;

3) подсоединение/отсоединение устройства ввода/вывода;

c) попытки неавторизованного доступа, такие как:

1) неудавшиеся или отклоненные действия пользователей;

2) неудавшиеся или отклоненные действия, затрагивающие данные или другие ресурсы;

3) нарушения политики доступа и уведомления сетевых шлюзов и межсетевых экранов;

4) предупреждения от собственных систем обнаружения вторжения;

d) предупреждения или отказы системы, такие как:

1) предупреждения или сообщения пульта управления;

2) изъятие системного журнала;

3) предупредительные сигналы, связанные с управлением сетью;

4) предупредительные сигналы, подаваемые системой управления доступом;

e) изменения или попытки изменить параметры настройки системы безопасности и мер и средств контроля и управления.

Как часто следует анализировать результаты мониторинга деятельности, должно зависеть от возможных рисков информационной безопасности. Подлежащие рассмотрению факторы риска включают в себя:

a) критичность процессов, которые поддерживаются прикладными программами;

b) ценность, чувствительность и критичность затрагиваемой информации;

c) предшествующий случай проникновения и неправильного использования системы, а также частота использования уязвимостей;

d) степень взаимосвязи систем (особенно с общедоступными сетями);

e) деактивацию средств регистрации.

Процедуры мониторинга использования систем нужны для обеспечения уверенности в том, что пользователи выполняют только те действия, которые были явно разрешены.

Анализ журнала регистрации способствует пониманию угроз, с которыми сталкивается система, и каким образом они могут возникать.

Защита информации журналов регистрации

Средства регистрации и информацию журналов регистрации следует защищать от повреждения и неавторизованного доступа.

Рекомендация по реализации

Использование мер и средств контроля и управления должно быть нацелено на защиту от неавторизованных изменений и эксплуатационных проблем средств регистрации, включая:

a) изменения типов записываемых сообщений;

b) редактирование или удаление файлов журнала регистрации;

c) превышение объема памяти носителя, содержащего файл журнала регистрации, что может приводить либо к отказу регистрировать события, либо к затиранию информации о событиях, зарегистрированных в последнюю очередь.

Архивация некоторых контрольных журналов может требоваться как часть политики хранения записей или вследствие требований собирать и хранить доказательство.

Системные журналы часто содержат большой объем информации, значительная часть которой не представляет интереса сточки зрения мониторинга безопасности. Чтобы помочь в выявлении значимых событий в целях мониторинга безопасности, необходимо рассмотреть возможность автоматической записи соответствующих типов сообщений в отдельный журнал регистрации и (или) использования подходящих системных утилит или инструментальных средств аудита для осуществления контрольного считывания и оптимизации файла.

Системные журналы необходимо защищать, так как если данные в них модифицированы или удалены, то они могут создавать ложное чувство безопасности.

Журналы регистрации администратора и оператора

Действия системного администратора и системного оператора следует регистрировать.

Журналы регистрации должны содержать:

a) время, когда произошло событие (успешное или неуспешное);

b) информацию о событии (например обработанные файлы) или об отказе (например произошла ошибка и было предпринято корректирующее действие);

c) учетную запись и имя администратора или оператора, сделавшего ее;

d) перечень задействованных процессов.

Анализ журналов регистрации системного администратора и оператора следует проводить на регулярной основе.

Система обнаружения вторжения, менеджмент которой осуществляется вне рамок контроля системных и сетевых администраторов, может быть использована для осуществления мониторинга действий системного и сетевого администрирования на предмет соответствия.

Регистрация неисправностей

Неисправности следует регистрировать, анализировать, и предпринимать в их отношении необходимые действия.

Неисправности, о которых стало известно от пользователей или посредством системных программ, имеющих отношение к проблемам, связанным с системами обработки информации или коммуникационными системами, необходимо регистрировать. Должны существовать четкие правила обработки неисправностей, включая:

a) анализ журналов регистрации неисправностей для обеспечения уверенности в том, что неисправности были соответствующим образом устранены;

b) анализ корректирующих мероприятий для обеспечения уверенности в том, что меры и средства контроля и управления не были скомпрометированы и что предпринятое действие полностью авторизовано.

Должна обеспечиваться уверенность в том, что регистрация ошибок становится возможной, если данная системная функция доступна.

Регистрация ошибок и неисправностей может влиять на производительность системы. Разрешение на такую регистрацию следует давать компетентному персоналу, а уровень регистрации, требуемый для отдельных систем, должен определяться оценкой рисков, с учетом снижения производительности.

Синхронизация часов

Часы во всех соответствующих системах обработки информации в пределах организации или домена безопасности должны быть синхронизированы с установленным источником точного времени.

Рекомендация по реализации

Если компьютер или устройство связи имеет возможность использовать часы, работающие в реальном времени, то эти часы должны быть установлены по согласованному нормативу, т е. всемирного координированного времени или местного стандартного времени. Поскольку некоторые часы, как известно, со временем начинают "спешить" или "отставать", должна существовать процедура, которая выявляет и исправляет любые значимые отклонения.

Правильная интерпретация формата дата/время важна для обеспечения уверенности в том, что временная отметка отражает реальную дату/время. Необходимо учитывать местную специфику (например переход на "летнее время").

Правильная установка компьютерных часов важна для обеспечения точности данных в контрольных журналах, которые могут потребоваться для расследований или в качестве доказательства в правовых (судебных) или дисциплинарных административных делах. Неаккуратные контрольные журналы могут затруднять такие расследования и дискредитировать эти доказательства. Часы, настроенные в соответствии с сигналами национальных атомных часов, передаваемыми по радио, могут использоваться как главные часы для настройки систем регистрации. Протокол сетевого времени может использоваться для поддержания всех серверов в состоянии, синхронизированном с главными часами.