Тема: Приобретение, разработка и эксплуатация информационных систем

1 Требования безопасности информационных систем

Цель: Обеспечить уверенность в том, что безопасность является неотъемлемой частью информационных систем.

Информационные системы включают эксплуатируемые системы, инфраструктуру, прикладные программы бизнеса, готовые продукты, услуги и прикладные программы, разработанные пользователями. Проектирование и внедрение информационной системы, поддерживающей процесс бизнеса, может быть критичным с точки зрения безопасности. Требования безопасности следует выявлять и согласовывать до разработки и (или) внедрения информационных систем.

Все требования безопасности следует выявлять на стадии определения задач проекта, а также обосновывать, согласовывать и документально оформлять в рамках общего проекта по внедрению информационной системы.

Анализ требований безопасности и спецификация

Мера и средство контроля и управления

Необходимо, чтобы в формулировках требований бизнеса для новых информационных систем или при модернизации существующих информационных систем были определены требования к мерам и средствам контроля и управления безопасности.

Рекомендация по реализации

В спецификациях требований к мерам и средствам контроля и управления следует учитывать как встроенные в информационную систему автоматизированные меры и средства контроля и управления, так и необходимость поддержки ручного управления. Аналогично следует подходить к оценке пакетов прикладных программ, разработанных или приобретенных для прикладных программ бизнеса.

Необходимо, чтобы требования безопасности и соответствующие меры и средства контроля и управления отражали ценность информационных активов (см. 7.2) и потенциальный ущерб бизнесу, который мог бы явиться результатом недостаточности мер безопасности или их отсутствия.

Системные требования в отношении информационной безопасности и процессов реализации безопасности необходимо включать на ранних стадиях проектов, касающихся информационных систем. Определение мер и средств контроля и управления на стадии проектирования системы позволяет существенно снизить затраты на их внедрение и поддержку по сравнению с разработкой мер и средств контроля и управления во время или после внедрения системы.

В случае приобретения готовых продуктов необходимо соблюдение формального процесса приобретения и тестирования. В договорах с поставщиками должны учитываться определенные требования безопасности. Если функциональность безопасности в предлагаемом готовом продукте не удовлетворяет установленному организацией требованию, то тогда необходимо повторно рассмотреть порождаемый этим фактом риск и связанные с ним меры и средства контроля и управления прежде, чем продукт будет приобретен. Если обеспечивается дополнительная функциональность, и это создает риск безопасности, то ее следует блокировать, или пересмотреть предлагаемую структуру управления, чтобы определить возможность использования преимуществ имеющейся дополнительной функциональности.

2 Корректная обработка в прикладных программах

Цель: Предотвратить ошибки, потерю, неавторизованную модификацию или нецелевое использование информации в прикладных программах.

Соответствующие меры и средства контроля и управления необходимо предусмотреть в прикладных программах, включая прикладные программы, разработанные пользователем, для обеспечения уверенности в корректности обработки данных. Указанные меры и средства контроля и управления должны также включать возможность подтверждения корректности ввода, обработки и вывода данных.

Дополнительные меры и средства контроля и управления могут потребоваться для систем, которые обрабатывают или оказывают воздействие на чувствительную, ценную или критическую информацию. Такие меры и средства контроля и управления безопасности должны быть определены на основе требований безопасности и оценки рисков.

Подтверждение корректности входных данных

Мера и средство контроля и управления

Входные данные для прикладных программ должны проходить процедуру подтверждения с целью обеспечения уверенности в их корректности и соответствии.

Проверки следует проводить при вводе транзакций бизнеса, справочников (например имена и адреса, кредитные лимиты, идентификационные номера клиентов) и таблиц параметров (например цены продаж, курсы валют, ставки налогов).

Необходимо рассмотреть следующие рекомендации:

a) двойной ввод или другие процедуры проверки ввода, например проверка границ или ограничение полей до определенных диапазонов вводимых данных с целью обнаружения следующих ошибок:

1) значений, выходящих за допустимый диапазон;

2) недопустимых символов в полях данных;

3) отсутствующих или неполных данных;

4) превышения верхних и нижних пределов объема данных;

5) запрещенных или противоречивых контрольных данных;

b) периодическая проверка содержимого ключевых полей или файлов данных для подтверждения их достоверности и целостности;

c) сверка печатных копий вводимых документов на предмет выявления любых несанкционированных изменений (необходимо, чтобы все изменения во вводимых документах были утверждены);

d) процедуры реагирования на ошибки проверки;

e) процедуры проверки достоверности вводимых данных;

f) определение обязанностей всех сотрудников, вовлеченных в процесс ввода данных;

g) создание журнала регистрации действий, связанных с процессом ввода данных

Там, где это целесообразно, можно рассмотреть автоматическую экспертизу и проверку вводимых данных, чтобы снизить риск ошибок и предотвратить стандартные атаки, включая переполнение буфера и внесение кода.

Управление внутренней обработкой

Мера и средство контроля и управления

Подтверждающие проверки должны быть включены в прикладные программы с целью обнаружения любого искажения информации вследствие ошибок обработки или преднамеренных действий.

Разработка и реализация прикладных программ должны обеспечивать уверенность в том, что риски обработки сбоев, ведущих к потере целостности, сведены к минимуму.

Необходимо учитывать, в частности, следующее:

a) использование функций добавления, модификации и удаления для осуществления изменений данных;

b) процедуры, не допускающие запуск программ, исполняемых в неправильной последовательности или исполняемых после сбоя в предшествующей обработке;

c) использование соответствующих программ для восстановления после сбоев и обеспечение правильной обработки данных;

d) защиту от атак, использующих перегрузки/переполнения буфера.

Необходимо подготавливать соответствующую технологическую карту, действия документально оформлять и надежно хранить результаты. Примеры проверок, которые могут быть комбинированными, включают следующее:

a) контроль сеансовой или пакетной обработки с целью согласования остатков массива данных после обновлений в результате транзакции;

b) контроль баланса, чтобы проверить соответствие открываемых данных и данных предыдущего закрытия, а именно:

1) меры и средства контроля и управления "от-выполнения-к-выполнению";

2) суммарное количество обновлений файла;

3) контроль "от-программы-к-программе";

c) подтверждение корректности данных, сгенерированных системой ;

d) проверки целостности, аутентичности или какого-либо другого свойства безопасности, полученных данных или программного обеспечения, или передаваемых между центральным и удаленными компьютерами;

e) контрольные суммы записей и файлов;

f) проверки для обеспечения уверенности в том, что прикладные программы выполняются в нужное время;

g) проверки для обеспечения уверенности в том, что прикладные программы выполняются в правильном порядке и прекращают работу в случае отказа, и что дальнейшая обработка приостанавливается до тех пор, пока проблема не будет разрешена;

h) создание журнала регистрации действий, связанных с обработкой

Данные, которые были введены правильно, могут быть искажены вследствие аппаратных ошибок, ошибок обработки или преднамеренных действий. Обоснование необходимых проверок зависит от характера прикладной программы и влияния на бизнес любого искажения данных.

Целостность сообщений

Мера и средство контроля и управления

Необходимо определить требования в отношении обеспечения аутентичности и защиты целостности сообщений в прикладных программах, а также идентифицировать и внедрить соответствующие меры и средства контроля и управления.

Следует проводить оценку рисков безопасности для определения необходимости обеспечения целостности сообщений, и идентификации соответствующего способа реализации.

Криптографические методы могут использоваться как соответствующее средство реализации аутентификации сообщений.

Подтверждение выходных данных

Данные, выводимые из прикладной программы, должны быть проверены с целью обеспечения уверенности в корректности обработки хранимой информации и соответствия требованиям.

Проверка выходных данных может включать:

a) проверки достоверности с целью определения приемлемости выходных данных;

b) контрольная сверка результатов, для обеспечения уверенности в том, что все данные были обработаны;

c) предоставление достаточной информации для чтения или последующей системы обработки, чтобы определить корректность, полноту, точность и классификацию информации;

d) процедуры реагирования на проверку пригодности выходных данных;

e) определение обязанностей всех сотрудников, вовлеченных в процесс вывода данных;

f) создание журнала регистрации действий по подтверждению корректности выходных данных.

Как правило, системы и прикладные программы построены на предпосылке, что при наличии соответствующих подтверждений корректности, проверок и тестирования, выводимые данные будут всегда правильны. Но это не всегда так, т.е. при некоторых обстоятельствах, протестированные системы будут по-прежнему производить некорректные данные вывода.

3 Криптографические меры и средства контроля и управления

Цель: Защищать конфиденциальность, аутентичность или целостность информации, используя криптографические средства.

Необходимо разработать политику в отношении использования криптографических мер и средств контроля и управления. Для поддержки использования криптографических методов следует применять управление ключами.

Политика использования криптографических мер и средств контроля и управления

Мера и средство контроля и управления

В целях защиты информации необходимо разработать и реализовать политику в отношении использования криптографических мер и средств контроля и управления.

При разработке криптографической политики необходимо учитывать следующее:

a) позицию руководства в отношении использования средств криптографии во всей организации, включая общие принципы, в соответствии с которыми должна быть защищена бизнес-информация ;

b) основанный на оценке риска требуемый уровень защиты, который должен быть определен с учетом типа, стойкости и качества требуемого алгоритма шифрования;

c) использование шифрования для защиты чувствительной информации, передаваемой с помощью переносных или сменных носителей и устройств или по линиям связи;

d) подход к управлению ключами, включая методы по защите криптографических ключей и восстановлению зашифрованной информации в случае потери, компрометации или повреждения ключей;

e) роли и обязанности, например персональная ответственность за:

1) внедрение политики;

2) управление ключами, включая генерацию ключей;

f) стандарты, которые должны быть приняты для эффективной реализации во всей организации (какое решение используется и для каких процессов бизнеса);

g) влияние использования зашифрованной информации на меры и средства контроля и управления, которые базируются на проверки содержимого (например обнаружение вирусов).

При внедрении политики организации в области криптографии следует учитывать требования законодательства и ограничения, которые могут применяться в отношении криптографических методов в различных странах, а также вопросы трансграничного потока зашифрованной информации

Криптографические меры и средства контроля и управления могут использоваться для достижения различных целей безопасности, например:

a) конфиденциальности посредством использования шифрования информации для защиты чувствительной или критической информации как хранимой, так и передаваемой;

b) целостности/аутентичности посредством использования цифровых подписей или кодов аутентификации сообщений для защиты аутентичности и целостности, хранимой или передаваемой чувствительной или критической информации;

c) неотказуемости, посредством использования криптографических методов для получения подтверждения того, что событие или действие имело или не имело место.

Процесс принятия решения относительно использования криптографии следует рассматривать в рамках более общего процесса оценки рисков и выбора мер и средств контроля и управления. Такая оценка может затем использоваться для определения того, является ли криптографическая мера и средство контроля и управления подходящей, какой тип мер и средств контроля и управления следует применять, с какой целью и для каких процессов бизнеса.

Политика использования криптографических мер и средств контроля и управления необходима для того, чтобы максимизировать выгоду и минимизировать риски использования криптографических методов, и чтобы избежать неадекватного или неправильного использования данных средств. При использовании цифровых подписей, необходимо учитывать все применимые требования законодательства, в особенности законодательных актов, описывающих условия, при которых цифровая подпись имеет юридическую силу

Мера и средство контроля и управления

Для поддержки использования организацией криптографических методов необходимо применять управление ключами.

Все криптографические ключи следует защищать от модификации, потери и разрушения. Кроме того, секретным и персональным ключам необходима защита от несанкционированного раскрытия. Оборудование, используемое для генерации, хранения и архивирования ключей должно быть физически защищено.

Система управления ключами должна быть основана на согласованном множестве стандартов, процедур и безопасных методов для:

a) генерации ключей для различных криптографических систем и прикладных программ;

b) генерации и получения сертификатов открытых ключей;

c) рассылки ключей предполагаемым пользователям, включая инструкции по активации указанных ключей при получении;

d) хранения ключей, в том числе инструкций в отношении получения доступа к ключам авторизованных пользователей;

e) замены или обновления ключей, включая правила в отношении порядка и сроков замены ключей;

f) действий в отношении скомпрометированных ключей;

g) аннулирования ключей, в том числе порядок изъятия и деактивации, например в случае компрометации ключей или при увольнении пользователя из организации (при этом ключи необходимо также архивировать);

h) восстановления ключей, которые были утеряны или испорчены, как часть менеджмента непрерывности бизнеса, например для восстановления зашифрованной информации;

i) архивирования ключей, например для восстановления заархивированной или резервной информации;

j) уничтожения информации;

k) регистрации и аудита действий, связанных с управлением ключами.

Для уменьшения вероятности компрометации ключей необходимо, чтобы они имели определенные даты активации и деактивации. Данный период времени зависит от обстоятельств, при которых используются криптографические меры и средства контроля и управления, и от осознаваемого риска.

В дополнение к вопросу безопасности менеджмента секретных и персональных ключей, необходимо также учитывать вопросы аутентичности открытых ключей. Процесс аутентификации может осуществляться при использовании сертификатов открытых ключей, которые обычно выдаются органом сертификации, представляющим собой официально признанную организацию, применяющую соответствующие меры и средства контроля и управления и процедуры для обеспечения требуемой степени доверия.

Необходимо, чтобы соглашение об уровне обслуживания или договоры с внешними поставщиками услуг, связанных с криптографией, например с органом - держателем справочников сертификатов, включали положения относительно ответственности, надежности услуг и времени реагирования на запросы по их предоставлению

Управление криптографическими ключами является существенным аспектом для эффективного использования криптографических средств. Различаются два типа криптографических методов:

a) методы, применяемые в отношении секретных ключей, когда две или более стороны совместно используют один и тот же ключ, и этот ключ применяется как для шифрования, так и для дешифрования информации; данный ключ должен храниться в секрете, так как любой, имеющий доступ к этому ключу, может дешифровать всю информацию, зашифрованную с помощью этого ключа, или ввести несанкционированную информацию, используя этот ключ;

b) методы, применяемые в отношении открытых ключей, где каждый пользователь имеет пару ключей, открытый ключ (который может быть показан любому) и секретный ключ (который должен храниться в секрете); методы с открытыми ключами могут использоваться для проверки и формирования цифровых подписей

Существует угроза подделки цифровой подписи и замены открытого ключа пользователя на фальсифицированный. Данная проблема решается с помощью органов - держателей сертификатов открытых ключей.

Криптографические методы могут также использоваться и для защиты криптографических ключей. Может потребоваться наличие процедур для обработки запросов правоохранительных органов на получение криптографических ключей, например для представления зашифрованной информации в незашифрованном виде в качестве доказательства в суде.

4 Безопасность системных файлов

Цель: Обеспечить уверенность в безопасности системных файлов.

Доступ к системным файлам и исходным текстам программ следует контролировать, а проекты ИТ и деятельности по их поддержке необходимо осуществлять безопасным способом. Необходимо проявлять осторожность в среде тестирования, чтобы не подвергать риску чувствительную информацию.

Управление эксплуатируемым программным обеспечением

Мера и средство контроля и управления

Необходимо применять процедуры контроля установки программного обеспечения в эксплуатируемых системах.

Для сведения к минимуму риска повреждения эксплуатируемых систем необходимо учесть следующие рекомендации в отношении контроля изменений:

a) обновление эксплуатируемого программного обеспечения, прикладных программ и библиотек программ должны выполнять только обученные администраторы при наличии соответствующего разрешения руководства ;

b) эксплуатируемые системы должны содержать только утвержденный исполняемый программный код и не должны содержать коды разработки или компиляторы;

c) прикладные программы и программное обеспечение следует внедрять в эксплуатируемую систему только после всестороннего и успешного тестирования, которое должно выполняться на изолированных системах и включать в себя тесты на пригодность к эксплуатации, безопасность, влияние на другие системы и удобство для пользователя (см. 10.1.4); необходимо обеспечить уверенность в том, что все соответствующие библиотеки исходных текстов программ были обновлены;

d) меры и средства контроля и управления конфигурацией системы необходимо использовать согласно системной документации для сохранения управления всем реализуемым программным обеспечением;

e) прежде чем изменения будут реализованы, необходимо применять метод отката;

f) в контрольном журнале должны быть сохранены все обновления эксплуатируемой библиотеки программ;

g) предыдущие версии прикладного программного обеспечения следует сохранять на случай непредвиденных обстоятельств;

h) старые версии программного обеспечения следует архивировать вместе со всей требуемой информацией и параметрами, процедурами, конфигурационными деталями и поддерживающим программным обеспечением до тех пор, пока данные хранятся в архиве.

Необходимо, чтобы поставляемое поставщиком программное обеспечение, используемое в действующей системе, поддерживалось на уровне, обеспечиваемом поставщиком. Со временем поставщики программного обеспечения прекращают поддерживать более старые версии программного обеспечения. Организация должна учитывать риски, когда она полагается на неподдерживаемое программное обеспечение.

Любое решение об обновлении программного обеспечения до новой версии должно учитывать требования бизнеса в отношении изменения и безопасности новой версии, т.е. введение новых функциональных возможностей безопасности или количество и серьезность проблем безопасности, связанных с этой версией. Исправления (патчи) программного обеспечения следует применять, если они помогают удалять или снижать уязвимости безопасности

Физический или логический доступ следует предоставлять поставщикам только для целей поддержки, по мере необходимости и на основании разрешения руководства. Действия поставщика должны подвергаться мониторингу.

Программное обеспечение компьютеров может использовать поставляемые внешним (иностранным) поставщиком программное обеспечение и модули, которые должны быть контролируемы и управляемы во избежание несанкционированных изменений, которые могут способствовать нарушению безопасности.

Эксплуатируемую систему следует обновлять только при необходимости, например, если текущая версия эксплуатируемой системы больше не удовлетворяет требованиям бизнеса. Обновление не следует проводить только потому, что доступна новая версия для эксплуатируемой системы. Новые версии систем, находящихся в промышленной эксплуатации, могут быть менее безопасными, менее стойкими и менее понятными, чем текущие системы.

Защита тестовых данных системы

Мера и средство контроля и управления

Данные тестирования следует тщательно отбирать, защищать и контролировать.

Следует избегать использования действующих баз данных, содержащих персональную или какую-либо другую чувствительную информацию, для целей тестирования. Если персональная или какая-либо другая чувствительная информация требуется для тестирования, то все чувствительные подробности и информационное наполнение следует удалить или изменить до неузнаваемости перед использованием.

Для защиты действующих (рабочих) данных, если они используются для целей тестирования, необходимо применять следующие рекомендации:

a) процедуры управления доступом, применимые для эксплуатируемых прикладных систем, следует также применять и для тестирования прикладных систем;

b) необходимо отдельное разрешение на каждый случай копирования действующей (рабочей) информации для тестирования прикладной системы;

c) после того как тестирование было завершено, действующую (рабочую) информацию следует немедленно удалить из тестируемой прикладной системы;

d) копирование и использование действующей (рабочей) информации должно фиксироваться для обеспечения контрольной записи.

Для осуществления системного или приемочного тестирования обычно требуется существенный объем тестовых данных, которые максимально приближены к действующим (рабочим) данным.

Управление доступом к исходным текстам программ

Мера и средство контроля и управления

Доступ к исходным текстам программ необходимо ограничивать.

В целях предотвращения введения несанкционированных функциональных возможностей и во избежание непреднамеренных изменений должен быть обеспечен строгий контроль доступа к исходным текстам программ и связанным с ними документам (например проектам, спецификациям, планам верификации и планам валидации). В отношении исходных текстов программ это может быть достигнуто с помощью контролируемого централизованного хранения таких текстов, предпочтительнее в библиотеках исходных текстов программ.

Чтобы сократить возможность искажения компьютерных программ, необходимо рассмотреть следующие рекомендации по управлению доступом к таким библиотекам исходных текстов программ:

a) по возможности, следует избегать хранения библиотек исходных текстов программ в эксплуатируемых системах;

b) менеджмент исходных текстов программ и библиотек исходных текстов программ следует осуществлять в соответствии с установленными процедурами;

c) персонал поддержки не должен иметь неограниченный доступ к библиотекам исходных текстов программ;

d) обновление библиотек исходных текстов программ и связанных с ними элементов, а также предоставление программистам исходных текстов программ должны осуществляться только после получения соответствующего разрешения;

e) распечатки (листинги) программ следует хранить безопасным образом ;

f) в контрольном журнале должны фиксироваться все обращения к библиотекам исходных текстов программ;

g) поддержку и копирование библиотек исходных текстов программ следует осуществлять в соответствии со строгими процедурами контроля изменений .

Безопасность в процессах разработки и поддержки

Цель: Поддерживать безопасность прикладных систем и информации.

Необходимо строго контролировать среды проектирования и поддержки

Необходимо, чтобы руководители, ответственные за прикладные системы, также несли ответственность и за безопасность среды проектирования или поддержки. Они должны обеспечить уверенность в том, что все предложенные изменения системы проанализированы на предмет возможных нарушений безопасности системы или условий эксплуатации.

Процедуры управления изменениями

Мера и средство контроля и управления

Внесение изменений следует контролировать, используя формальные процедуры управления изменениями.

Для сведения к минимуму повреждений информационных систем следует осуществлять и документально оформлять формальные процедуры контроля изменений. Введение новых и значительные изменения существующих систем должны сопровождаться формальным процессом документального оформления, детализирования, тестирования, контроля качества и управляемого внедрения.

Указанный процесс должен включать в себя оценку рисков, анализ влияния изменений и детализацию необходимых мер и средств контроля и управления безопасности. Он также должен обеспечивать уверенность в том, что не нарушены безопасность и сами процедуры управления, что программистам, отвечающим за поддержку, предоставлен доступ только к тем частям системы, которые необходимы для их работы, и что любые изменения формально согласованы и одобрены.

По возможности, прикладные программы и эксплуатационные процедуры управления изменениями должны быть интегрированы. Процедуры изменения должны включить:

a) ведение учета согласованных уровней разрешений;

b) обеспечение уверенности в том, что изменения представлены уполномоченными пользователями;

c) анализ мер и средств контроля и управления, а также процедур целостности на предмет обеспечения уверенности в том, что они не будут нарушены изменениями;

d) выявление всего программного обеспечения, информации, объектов баз данных и аппаратных средств, требующих изменений;

e) получение формального одобрения на детальные предложения по изменениям перед началом работы;

f) обеспечение уверенности в том, что авторизованный пользователь одобрил все изменения до их реализации;
g) обеспечение уверенности в том, что комплект системной документации обновляется после завершения каждого изменения, и что старая документация архивируется или удаляется;
h) поддержание управления версиями для всех обновлений программного обеспечения;
i) сохранение контрольных записей обо всех запросах на изменение;
j) обеспечение уверенности в том, что эксплуатационная документация (см. 10.1.1) и пользовательские процедуры при необходимости изменяются, чтобы соответствовать внесенным изменениям;
к) обеспечение уверенности в том, что процесс внедрения изменений осуществляется в согласованное время и не нарушает затрагиваемых процессов бизнеса.

Общепринятая практика включает в себя тестирование нового программного обеспечения в среде, которая отделена от среды эксплуатации и среды разработки. Это обеспечивает средства контроля над новым программным обеспечением, и предоставляет дополнительную защиту действующей (рабочей) информации, используемой в целях тестирования. Для этих целей следует использовать изменения (патчи), служебные пакеты обновлений и другие обновления. Автоматические обновления не следует применять в критических системах, поскольку некоторые обновления могут являться причиной отказа критических прикладных программ.

Техническая проверка прикладных программ после изменений эксплуатируемой системы

Мера и средство контроля и управления

При внесении изменений в эксплуатируемые системы прикладные программы, имеющие большое значение для бизнеса, следует анализировать и тестировать с целью обеспечения уверенности в том, что не оказывается неблагоприятного воздействия на функционирование или безопасность организации.

Этот процесс должен охватывать:

a) анализ мер и средств контроля и управления прикладными программами и процедур целостности на предмет обеспечения уверенности в том, что они не будут нарушены изменениями эксплуатируемой системы;

b) обеспечение уверенности в том, что ежегодный план поддержки и бюджет предусматривает анализ и тестирование систем, необходимые при изменениях эксплуатируемой системы;

c) обеспечение уверенности в том, что уведомления об изменениях эксплуатируемой системы поступают своевременно, чтобы дать возможность перед их реализацией провести соответствующие тесты и анализы;

d) обеспечение уверенности в том, что соответствующие изменения вносятся в планы обеспечения непрерывности бизнеса.

Определенной группе лиц или отдельному специалисту следует вменять в обязанность проведение мониторинга уязвимостей, версий патчей поставщиков и их установок

Ограничения на изменения пакетов программ

Мера и средство контроля и управления

Необходимо избегать модификаций пакетов программ, ограничиваться необходимыми изменениями и строго контролировать все сделанные изменения.

Насколько возможно и допустимо с практической точки зрения, пакеты программ, поставляемые поставщиком, следует использовать без изменений. Там, где необходимо внести изменения в пакет программ, следует учитывать следующее:

a) риск в отношении встроенных мер и средств контроля и управления и процедур обеспечения целостности;

b) необходимость получения согласия поставщика;

c) возможность получения требуемых изменений от поставщика в качестве стандартной программы обновления;

d) возможные последствия в случае, если организация станет ответственной за будущее сопровождение программного обеспечения в результате внесенных изменений.

Если необходимо внесение изменений, то оригинальное программное обеспечение следует сохранить, а изменения вносить в четко определенную копию. Следует реализовывать процесс управления обновлением программного обеспечения, чтобы иметь уверенность в том, что для всего разрешенного программного обеспечения устанавливаются новейшие одобренные к применению патчи и обновления прикладных программ. Все изменения необходимо полностью тестировать и документально оформлять таким образом, чтобы их можно было использовать повторно для будущих обновлений программного обеспечения. При необходимости изменения должны быть проверены и подтверждены независимой оценочной организацией.

Утечка информации

Мера и средство контроля и управления

Возможность утечки информации должна быть предотвращена.

Для снижения риска утечки информации, например по причине использования и эксплуатации скрытых каналов, необходимо принимать во внимание следующее:

a) сканирование носителей исходящей информации и каналов связи на наличие скрытой информации;

b) маскирование и регулирование поведения систем и каналов связи для снижения вероятности того, что третья сторона сможет извлечь информацию из поведения систем и каналов связи;

c) использование систем и программного обеспечения, которые считаются максимально достоверными, например использование оцененных продуктов;

d) регулярный мониторинг деятельности персонала и систем там, где это разрешено существующим законодательством или предписаниями;

Скрытые каналы -это каналы, не предназначенные для передачи информационных потоков, но которые, тем не менее, могут существовать в системе или сети. Например манипулирование битами в пакетах протоколов связи может использоваться как скрытый метод передачи сигналов. Природа скрытых каналов такова, что предотвратить существование всех возможных скрытых каналов затруднительно или даже невозможно. Однако такие каналы часто используются "троянскими" программами. Следовательно, принятие мер по защите от "троянских" программ снижает риск использования скрытых каналов.

Предотвращение неавторизованного доступа к сети, а также политики и процедуры, препятствующие неправильному использованию информационных услуг персоналом, способствуют защите от скрытых каналов.

Аутсорсинг разработки программного обеспечения

Мера и средство контроля и управления

Аутсорсинг разработки программного обеспечения должен быть под наблюдением и контролем организации.

Там, где для разработки программного обеспечения привлекается сторонняя организация, необходимо учитывать следующее:

a) лицензионные соглашения, права собственности на программы и права интеллектуальной собственности;

b) сертификацию качества и точности выполненной работы;

c) соглашения условного депонирования на случай отказа сторонней организации выполнять свои обязательства;

d) права доступа с целью проверки качества и точности сделанной работы;

e) договорные требования к качеству и функциональной безопасности программ;

f) тестирование программ перед установкой на предмет обнаружения вредоносных и "троянских" программ

6 Менеджмент технических уязвимостей

Цель: Снизить риски, являющиеся результатом использования опубликованных технических уязвимостей.

Менеджмент технических уязвимостей следует осуществлять эффективным, систематическим и повторяемым способом, с проведением измерений с целью подтверждения его эффективности

Эти соображения должны касаться эксплуатируемых систем и любых других используемых прикладных программ.

Управление техническими уязвимостями

Мера и средство контроля и управления

Необходимо получать своевременную информацию о технических уязвимостях используемых информационных систем, оценивать незащищенность организации в отношении таких уязвимостей и принимать соответствующие меры для рассмотрения связанного с ними риска.

Постоянно обновляемая и полная опись активов является предпосылкой эффективного менеджмента технических уязвимостей. Специальная информация, необходимая для поддержки менеджмента технических уязвимостей, включает в себя информацию о поставщике программного обеспечения, номерах версий, текущем состоянии развертывания (например какое программное обеспечение установлено на каких системах) и специалисте(ах), отвечающем(их) в организации за программное обеспечение.

Аналогично, своевременное действие должно предприниматься в ответ на выявление потенциальных технических уязвимостей. Для создания эффективного процесса менеджмента в отношении технических уязвимостей необходимо выполнять следующие рекомендации:

a) в организации необходимо определять и устанавливать роли и обязанности, связанные с менеджментом технических уязвимостей, включая мониторинг уязвимостей, оценку риска проявления уязвимостей, исправление программ (патчинг), слежение за активами и любые другие координирующие функции;

b) информационные ресурсы, которые будут использоваться для выявления значимых технических уязвимостей и обеспечения осведомленности о них, следует определять для программного обеспечения и другой технологии на основе списка инвентаризации активов; эти информационные ресурсы должны обновляться вслед за изменениями, вносимыми в опись, или когда найдены другие новые или полезные ресурсы;

c) необходимо определить временные параметры реагирования на уведомления о потенциально значимых технических уязвимостях;

d) после выявления потенциальной технической уязвимости организация должна определить связанные с ней риски и действия, которые необходимо предпринять; такие действия могут включать внесение исправлений в уязвимые системы и (или) применение других мер и средств контроля и управления;

e) в зависимости от того, насколько срочно необходимо рассмотреть техническую уязвимость, предпринимаемое действие следует осуществлять в соответствии с мерами и средствами контроля и управления, связанными с менеджментом изменений, или следуя процедурам реагирования на инциденты информационной безопасности ;

f) если имеется возможность установки патча, следует оценить риски, связанные с его установкой (риски, создаваемые уязвимостью, необходимо сравнить с риском установки патча);

g) перед установкой патчи следует тестировать и оценивать для обеспечения уверенности в том, что они являются эффективными и не приводят к побочным эффектам, которые нельзя допускать; если нет возможности установить патч, следует рассмотреть другие меры и средства контроля и управления, например:

1) отключение сервисов, связанных с уязвимостью;

2) адаптацию или добавление средств управления доступом, например межсетевых экранов на сетевых границах;

3) усиленный мониторинг для обнаружения или предотвращения реальных атак;

4) повышение осведомленности об уязвимостях;

h) в контрольный журнал следует вносить информацию о всех предпринятых процедурах;

i) следует регулярно проводить мониторинг и оценку процесса менеджмента технических уязвимостей в целях обеспечения уверенности в его эффективности и действенности;

j) в первую очередь следует обращать внимание на системы с высоким уровнем риска.

Правильное функционирование процесса менеджмента технических уязвимостей играет важную роль для многих организаций, поэтому процесс должен подвергаться регулярному мониторингу. Для обеспечения уверенности в том, что потенциально значимые технические уязвимости выявлены, важна точная инвентаризация.

Менеджмент технических уязвимостей может рассматриваться как подфункция менеджмента изменений и в качестве таковой может воспользоваться процессами и процедурами менеджмента изменений.

Поставщики часто испытывают на себе значительное давление, заключающееся в требовании выпускать патчи в кратчайшие сроки. Поэтому патч не может решить проблему адекватно и может иметь побочные эффекты. К тому же, в некоторых случаях, если патч был однажды применен, деинсталлировать его может быть нелегко.

Если адекватное тестирование патчей провести не удается, например по причине затрат или отсутствия ресурсов, можно рассмотреть задержку в осуществлении внесения изменений, чтобы оценить связанные с этим риски, основанные на опыте других пользователей.