Тема: Управление доступом.

1. Требование бизнеса по управлению доступом

Доступ к информации, средствам обработки информации и процессам бизнеса должен быть управляемым с учетом требований бизнеса и безопасности.

Правила управления доступом должны учитывать политику в отношении распространения и авторизации информации.

Мера и средство контроля и управления

Политика управления доступом должна создаваться, документально оформляться и пересматриваться с учетом требований бизнеса и безопасности для доступа.

Рекомендация по реализации

Правила управления доступом и права каждого пользователя или группы пользователей должны быть четко сформулированы в политике управления доступом. Существует как логическое, так и физическое управление доступом (см. 9), и их следует рассматривать совместно. Пользователям и поставщикам услуг должны быть представлены четко сформулированные требования бизнеса, предъявляемые к управлению доступом.

Необходимо, чтобы в политике было учтено следующее:

a) требования в отношении безопасности конкретных прикладных программ бизнеса;

b) определение всей информации, связанной с прикладными программами бизнеса, и рисков, касающихся информации;

c) правила в отношении распространения информации и авторизации доступа, например необходимо знать принципы и уровни безопасности и классификации информации;

d) согласованность между управлением доступом и политиками классификации информации различных систем и сетей;

e) соответствующие требования законодательства и любые договорные обязательства в отношении защиты доступа к данным или услугам;

f) стандартные профили доступа пользователей для должностных ролей в организации;

g) менеджмент прав доступа в распределенной среде или сетях с учетом всех типов доступных соединений;

h) разделение ролей в отношении управления доступом, например запрос доступа, авторизация доступа, администрирование доступа;

i) требования в отношении формального разрешения запросов доступа;

j) требования в отношении периодического пересмотра управления доступом;

k) аннулирование прав доступа.

При определении правил управления доступом, следует принимать во внимание следующее:

a) различие между правилами, обязательными для исполнения, и рекомендациями, которые являются необязательными или обусловленными чем-либо;

b) установление правил, основанных на предпосылке "все в общем случае запрещено, пока явно не разрешено", а не на более слабом принципе "все в общем случае разрешено, пока явно не запрещено";

c) изменения в информационных метках, инициированных как автоматически средствами обработки информации, так и по усмотрению пользователя;

d) изменения в правах пользователя как устанавливаемые автоматически информационной системой, так и определенные администратором;

e) правила, которые требуют особого разрешения перед применением, а также те, которые не требуют разрешения.

2 Менеджмент доступа пользователей

Цель: Обеспечить уверенность в том, что доступ предоставлен авторизованным пользователям и предотвращен неавторизованный доступ к информационным системам.

Необходимо наличие формальных процедур по контролю предоставления прав доступа к информационным системам и услугам.

Процедуры должны охватывать все стадии жизненного цикла доступа пользователей, от начальной регистрации новых пользователей до окончательной отмены регистрации пользователей, которым больше не требуется доступ к информационным системам и услугам.

Особое внимание должно быть уделено, где это необходимо, контролю предоставления привилегированных прав доступа, которые позволяют пользователям изменять управление системой.

Необходима формальная процедура регистрации и снятия с учета пользователей в отношении предоставления и отмены доступа ко всем информационным системам и услугам.

Процедура управления доступом в отношении регистрации и снятия с учета пользователей должна включать:

a) использование уникальных идентификаторов пользователей, позволяющих отследить действия пользователей, чтобы они несли ответственность за свои действия; использование групповых идентификаторов следует разрешать только там, где это необходимо для бизнеса или по условиям эксплуатации, все это должно быть утверждено и документировано;

b) проверку того, что пользователь имеет разрешение владельца системы на использование информационной системы или услуги; наличие отдельного разрешения на право доступа от руководства также может быть уместным;

c) проверку того, что уровень предоставленного доступа соответствует целям бизнеса и согласуется с политикой безопасности организации, например не нарушает принципа разграничения обязанностей ;

d) предоставление пользователям письменного заявления об их правах доступа;

e) требование от пользователей подписать заявление о принятии условий доступа;

f) обеспечение уверенности в том, что поставщики услуг не предоставляют доступ, пока процедуры авторизации не завершены;

g) ведение формального учета всех лиц, зарегистрированных как пользователи услуг;

h) немедленную отмену или блокирование прав доступа пользователей, у которых изменились роль, или рабочее место, или уволившихся из организации;

i) периодическую проверку и удаление или блокирование избыточных пользовательских идентификаторов и учетных записей;

j) обеспечение того, чтобы избыточные пользовательские идентификаторы не были переданы другим пользователям.

Необходимо рассмотреть возможность создания ролей доступа пользователей, основанных на требованиях бизнеса, которые объединяют несколько прав доступа в типовые профили доступа пользователей. Управление запросами и пересмотром предоставления прав доступа легче осуществлять на уровне таких ролей, чем на уровне отдельных прав.

Необходимо рассмотреть возможность включения положений о соответствующих санкциях в случае попыток неавторизованного доступа в трудовые договора сотрудников и договора о предоставлении услуг.

Управление привилегиями

Мера и средство контроля и управления

Предоставление и использование привилегий необходимо ограничивать и контролировать.

Рекомендация по реализации

Необходимо, чтобы в многопользовательских системах, которые требуют защиты от неавторизованного доступа, предоставление привилегий контролировалось посредством формального процесса авторизации

Необходимо рассмотреть следующие меры:

a) определение привилегий доступа в отношении каждого системного продукта, например эксплуатируемой системы, системы управления базами данных, каждой прикладной программы и пользователей, которым эти привилегии должны быть предоставлены;

b) привилегии должны предоставляться пользователям на основании принципа необходимости и принципа "событие за событием" в соответствии с политикой управления доступом, т е. минимального требования для их функциональной роли, только при необходимости;

c) обеспечение процесса авторизации и регистрации в отношении всех предоставленных привилегий, привилегии не должны предоставляться до завершения процесса авторизации;

d) проведение политики разработки и использования стандартных системных утилит (скриптов), для того чтобы избежать необходимости предоставления привилегий пользователям;

e) поощрение разработки и использования программ, позволяющих избежать необходимости предоставления привилегий при их исполнении;

f) использование различных идентификаторов пользователей при работе в нормальном режиме и с использованием привилегий.

Неадекватное использование привилегий в отношении администрирования системы (любой возможности или средства информационной системы, которые позволяют пользователю обходить меры и средства контроля и управления системы или прикладных программ) может быть одной из главных причин отказа или нарушения работы систем.

Управление паролями пользователей

Мера и средство контроля и управления

Распределение паролей необходимо контролировать посредством формального процесса управления.

Процесс должен включать следующие требования:

a) пользователей необходимо обязать подписать заявление о сохранении личных паролей в тайне и сохранении групповых паролей исключительно в пределах членов данной группы; это заявление может быть включено в условия и положения занятости;

b) если пользователи самостоятельно управляют собственными паролями, им следует первоначально предоставить безопасный временный пароль, который подлежит немедленной принудительной замене после входа в систему;

c) создание процедур проверки личности пользователя, прежде чем ему будет предоставлен новый, заменяющий или временный пароль;

d) временные пароли следует выдавать пользователям безопасным способом, при этом необходимо избегать использования третьих сторон или незащищенного (открытого) текста сообщений электронной почты;

e) временные пароли должны быть уникальны для каждого пользователя и не должны быть легко угадываемыми;

f) пользователи должны подтверждать получение паролей;

g) пароли никогда не следует хранить в компьютерных системах в незащищенной форме;

h) пароли поставщика, установленные по умолчанию, необходимо изменить после инсталляции систем или программного обеспечения

Пароли являются распространенным средством подтверждения личности пользователя перед предоставлением ему доступа к информационной системе или услуге в соответствии с его авторизацией. При необходимости следует рассмотреть возможность использования других технологий для идентификации и аутентификации пользователей, таких как биометрия, например проверка отпечатков пальцев, проверка подписи, а также использование аппаратных средств идентификации, например смарт-карт.

Пересмотр прав доступа пользователей

Руководство должно осуществлять формальный процесс периодического пересмотра прав доступа пользователей.

При пересмотре прав доступа должны учитываться следующие рекомендации:

a) права доступа должны пересматриваться регулярно, например через шесть месяцев, и после любых изменений, таких как повышение/понижение в должности, или увольнения;

b) права доступа пользователей должны пересматриваться и переназначаться при переходе с одной работы на другую в пределах одной организации;

c) разрешения в отношении специальных привилегированных прав доступа должны пересматриваться через небольшие интервалы времени, например через три месяца;

d) предоставленные привилегии должны пересматриваться через равные интервалы времени для обеспечения уверенности в том, что не были получены неавторизованные привилегии;

e) изменения привилегированных учетных записей должны регистрироваться для периодического анализа.

С целью поддержания эффективного контроля над доступом к данным и информационным услугам необходимо регулярно пересматривать права доступа пользователей.

3 Обязанности пользователя

Цель: Предотвращение неавторизованного доступа пользователей, а также компрометации или кражи информации и средств обработки информации

Сотрудничество авторизованных пользователей - важный аспект эффективной безопасности.

Пользователи должны быть осведомлены о своих обязанностях в отношении поддержания эффективного управления доступом, в частности, в отношении паролей и безопасности оборудования, с которым они работают.

Следует внедрять политику "чистого стола" и "чистого экрана" в целях снижения риска неавторизованного доступа или повреждения бумажных документов, носителей информации и средств обработки информации.

Использование паролей

Мера и средство контроля и управления

Пользователи должны придерживаться общепринятой практики в области безопасности при выборе и использовании паролей.

Всем пользователям следует рекомендовать:

a) сохранять конфиденциальность паролей;

b) избегать записи паролей (например на бумаге, в файле программного обеспечения или карманных устройствах), если не может быть обеспечено безопасное хранение и способ хранения не утвержден;

c) изменять пароли всякий раз, когда появляется любой признак возможной компрометации системы или пароля;

d) выбирать качественные пароли с достаточно минимальной длиной, которые:

1) легко запомнить;

2) не подвержены угадыванию или вычислению с использованием персональной информации, связанной с владельцем пароля, например имен, номеров телефонов, дат рождения и т.д.;

3) не могут быть восстановлены по словарям (т.е., не содержат слов, содержащихся в словарях);

4) не содержат последовательных идентичных символов, и не состоят из полностью числовых или полностью буквенных групп;

e) изменять пароли через разные интервалы времени или после определенного числа обращений к системе (пароли для привилегированных учетных записей следует менять чаще, чем обычные пароли) и избегать повторного или циклического использования старых паролей;

f) изменять временные пароли при первом начале сеанса;

g) не включать пароли ни в какой автоматизированный процесс начала сеанса, например с использованием хранимых макрокоманд или функциональных клавиш;

h) не использовать коллективно индивидуальные пользовательские пароли;

i) не использовать один и тот же пароль для бизнеса и некоммерческих целей.

Если пользователи нуждаются в доступе к многочисленным услугам, системам или платформам и вынуждены использовать несколько разных паролей, они должны знать, что могут использовать единый качественный пароль для всех услуг при уверенности, что разумный уровень защиты для хранения пароля был создан в рамках каждой услуги, системы или платформы.

Особую осторожность следует соблюдать при менеджменте системы "справочного стола", имеющей дело с утерянными или забытыми паролями, поскольку это может быть средством атаки на систему паролей.

Оборудование пользователя, оставленное без присмотра

Мера и средство контроля и управления

Пользователи должны обеспечивать соответствующую защиту оборудования, оставленного без присмотра

Всем пользователям необходимо знать требования безопасности и процедуры в отношении защиты оставленного без присмотра оборудования, а также их обязанности по обеспечению такой защиты

Пользователям рекомендуется:

a) завершать активные сеансы по окончании работы, если отсутствует соответствующий механизм блокировки, например защищенная паролем экранная заставка;

b) завершить сеанс на системах мэйнфреймов, серверах и офисных персональных компьютерах, когда работа завершена (т.е. не только выключить экран персонального компьютера или терминал);

c) обеспечивать безопасность персональных компьютеров или терминалов от несанкционированного использования с помощью блокировки клавиатуры или эквивалентных средств контроля, например доступа по паролю, когда оборудование не используется.

Оборудование, установленное в пользовательских зонах, например рабочие станции или файловые серверы, может потребовать специальной защиты от несанкционированного доступа, если оно оставлено без присмотра на длительный период.

Политика "чистого стола" и "чистого экрана"

Необходимо принять политику "чистого стола" в отношении бумажных документов и сменных носителей данных, а также политику "чистого экрана" в отношении средств обработки информации.

Политика "чистого стола" и "чистого экрана" должна учитывать классификацию информации, законодательные и договорные требования, а также соответствующие риски и корпоративную культуру организации.

Необходимо рассмотреть следующие рекомендации:

a) носители (бумажные или электронные), содержащие чувствительную или критическую информацию бизнеса, когда они не используются, следует убирать и запирать (лучше всего, в несгораемый сейф или шкаф), особенно, когда помещение пустует;

b) компьютеры и терминалы, когда их оставляют без присмотра, следует выключать или защищать посредством механизма блокировки экрана или клавиатуры, контролируемого паролем, токеном или аналогичным механизмом аутентификации пользователя, а также необходимо применять кодовые замки, пароли или другие меры и средства контроля и управления в то время, когда эти устройства не используются;

c) необходимо обеспечить защиту пунктов приема/отправки корреспонденции, а также автоматических факсимильных аппаратов;

d) необходимо предотвращать несанкционированное использование фотокопировальных устройств и другой воспроизводящей техники (сканеров, цифровых фотоаппаратов);

e) документы, содержащие чувствительную или критическую информацию, необходимо немедленно изымать из принтеров.

Политика "чистого стола"/"чистого экрана" снижает риски несанкционированного доступа, потери и повреждения информации как во время рабочего дня, так и вне рабочего времени. Сейфы или другие формы средств безопасного хранения также могут защищать хранимую в них информацию от форс-мажорных обстоятельств, таких как пожар, землетрясение, наводнение или взрыв.

Стоит обратить внимание на использование принтеров с функцией ПИН-кода, тогда только инициаторы отправления на печать смогут получать свои распечатки, и только если они стоят рядом с принтером.

4 Управление доступом к сети

Цель: Предотвратить неавторизованный доступ к сетевым услугам.

Доступ к внутренним и внешним сетевым услугам должен быть контролируемым.

Это необходимо для получения уверенности в том, что пользователи, которые имеют доступ к сетям и сетевым услугам, не нарушают их безопасность, путем:

a) обеспечения соответствующих интерфейсов между сетью организации и сетями, принадлежащими другим организациям, и общедоступными сетями;

b) b) внедрения соответствующих механизмов аутентификации в отношении пользователей и оборудования;

c)) предписанного управления доступом пользователей к информационным услугам.

Политика использования сетевых услуг

Мера и средство контроля и управления

Пользователям следует предоставлять доступ только к тем услугам, на использование которых они были специально уполномочены.

Следует сформулировать политику относительно использования сетей и сетевых услуг.

В политике необходимо рассмотреть:

a) сети и сетевые услуги, к которым разрешен доступ;

b) процедуры авторизации для определения того, кому и к каким сетям и сетевым услугам разрешен доступ;

c) меры и средства контроля и управления, а также процедуры менеджмента по защите доступа к сетевым подключениям и сетевым услугам;

d) средства, используемые для осуществления доступа к сетям и сетевым услугам (например условия, обеспечивающие возможность доступа по коммутируемой телефонной линии к провайдеру Интернет-услуг или удаленной системе).

Политика использования сетевых услуг должна быть согласована с политикой управления доступом

Несанкционированные и незащищенные подключения к сетевым услугам могут затрагивать целую организацию. Мера и средство контроля и управления, в частности, важна для сетевых подключений к чувствительным или критическим прикладным программам бизнеса, или в отношении пользователей, находящихся в зонах высокого риска, например в общественных местах или за пределами организации, т е. в общественных или внешних зонах, которые находятся за пределами непосредственного управления и контроля безопасностью со стороны организации.

Аутентификация пользователей для внешних соединений

Мера и средство контроля и управления

Для управления доступом удаленных пользователей следует применять соответствующие методы аутентификации.

Аутентификация удаленных пользователей может быть достигнута при использовании, например методов, основанных на применении средств криптографии, аппаратных средств защиты (токенов) или протоколов "запрос-ответ". Примером возможной реализации таких методов могут служить различные решения в отношении виртуальных частных сетей. Выделенные частные линии могут также использоваться для обеспечения доверия к источнику подключений.

Процедуры, меры и средства контроля и управления обратного вызова, например использование модемов с обратным вызовом, могут обеспечить защиту от несанкционированных и нежелательных подключений к средствам обработки информации организации. Указанные меры позволяют произвести аутентификацию пользователей, пытающихся установить удаленную связь с сетью организации. При использовании данной меры и средства контроля и управления организации не следует применять сетевые сервисы, которые включают переадресацию вызова, или, если они это делают, то они должны отключить использование таких функций, чтобы избежать недостатков, связанных с переадресацией вызова. Процесс обратного вызова должен обеспечить уверенность в том, что фактическое разъединение происходит на стороне организации. В противном случае, удаленный пользователь может держать линию открытой, считая, что произошла проверка обратного вызова. Процедуры, меры и средства контроля и управления обратного вызова следует тщательного протестировать на предмет наличия такой возможности.

Аутентификация узла может служить альтернативным средством аутентификации групп удаленных пользователей там, где они подсоединены к безопасному компьютерному средству совместного использования. Для аутентификации узла могут применяться криптографические методы, основанные, например, на механизме сертификации. Это является частью некоторых решений, основанных на виртуальных частных сетях.

Должны быть реализованы дополнительные меры и средства контроля и управления аутентификацией для управления доступом к беспроводным сетям. В частности, необходимо проявлять особую осторожность при выборе мер и средств контроля и управления для беспроводных сетей по причине больших возможностей необнаруживаемого перехвата и ввода сетевого трафика.

Внешние соединения обеспечивают благоприятную возможность для несанкционированного доступа к информации бизнеса, например доступа с использованием методов соединения по телефонной линии. Существуют различные методы аутентификации, некоторые из которых обеспечивают больший уровень защиты, чем другие, например методы, основанные на использовании средств криптографии, могут обеспечить достаточно надежную защиту. Исходя из оценки риска, важно определить требуемый уровень защиты. Это необходимо для соответствующего выбора метода аутентификации.

Наличие возможности автоматического подсоединения к удаленному компьютеру - это один из способов получения несанкционированного доступа к прикладной программе бизнеса. Это особенно важно, если для подсоединения используется сеть, которая находится вне сферы контроля менеджмента безопасности организации.

Идентификация оборудования в сетях

Мера и средство контроля и управления

Автоматическую идентификацию оборудования необходимо рассматривать как средство для аутентификации подсоединений, осуществляемых с определенных мест или определенного оборудования.

Идентификацию оборудования можно применять в тех случаях, когда важно, чтобы связь могла быть инициирована только с определенного места или оборудования. Для того чтобы показать, разрешено ли этому оборудованию подсоединение к сети, может быть использован внутренний или прикрепленный к оборудованию идентификатор. Такие идентификаторы должны четко показывать, к какой сети разрешено подключать оборудование, если эта сеть не единственная и, особенно, если эти сети имеют разную степень чувствительности. Для обеспечения безопасности идентификатора оборудования может возникнуть необходимость физической защиты оборудования.

Эти меры и средства контроля и управления могут быть дополнены другими методами, направленными на аутентификацию пользователя оборудования. Идентификация оборудования может применяться дополнительно к аутентификации пользователя.

Защита портов дистанционной диагностики и конфигурации

Мера и средство контроля и управления

Физический и логический доступ для портов дистанционной диагностики и конфигурации должен быть контролируемым и управляемым.

Рекомендация по реализации

Возможные меры и средства контроля и управления доступом к портам дистанционной диагностики и конфигурации включают в себя использование блокировки клавиш и поддерживающих процедур для контроля физического доступа к порту. Примером такой поддерживающей процедуры является обеспечение уверенности в том, что доступ к портам дистанционной диагностики и конфигурации осуществляется только при условии взаимной договоренности между руководителем, отвечающим за предоставление компьютерных услуг, и персоналом по поддержке аппаратных/программных средств.

Порты, сервисы и аналогичные средства, установленные на компьютере или сетевом оборудовании, которые определенно не требуются для функциональности бизнеса, следует блокировать или удалять.

Многие компьютерные системы, сетевые системы и системы связи внедряются со средствами удаленной диагностики или конфигурации для использования инженерами по обслуживанию. Будучи незащищенными, эти диагностические порты предоставляют возможность неавторизованного доступа.

Разделение в сетях

Мера и средство контроля и управления

Группы информационных услуг, пользователей и информационных систем в пределах сети должны быть разделены.

Один из методов контроля безопасности больших сетей состоит в том, чтобы разделить их на отдельные логические сетевые домены, например на внутренние сетевые домены организации и внешние сетевые домены, каждый из которых защищен определенным периметром безопасности. Совокупность последовательных мер и средств контроля и управления может быть применена в различных логических сетевых доменах для дальнейшего разделения среды сетевой безопасности, например общедоступные системы, внутренние сети и критические активы. Домены должны определяться на основе оценки риска и различных требований в отношении безопасности в пределах каждого из доменов.

Такой сетевой периметр может быть реализован посредством внедрения шлюза безопасности между двумя связанными сетями для управления доступом и информационным потоком между двумя доменами. Данный шлюз следует конфигурировать для фильтрации трафика между доменами и для блокирования несанкционированного доступа в соответствии с политикой организации по управлению доступом. Примером шлюза такого типа является межсетевой экран. Другим методом разделения отдельных логических доменов является ограничение сетевого доступа при использовании виртуальных частных сетей для групп пользователей в пределах организации.

Сети также могут быть разделены с помощью функциональных возможностей сетевых устройств, например IP-коммутации *(6). Отдельные домены могут быть, кроме того, реализованы посредством управления потоками сетевых данных при использовании возможностей маршрутизации/коммутации, например списков управления доступом.

Критерии для разделения сетей на домены следует основывать на политике управления доступом и требованиях к доступу с учетом влияния на относительную стоимость и производительность включения соответствующей технологии маршрутизации сетей и шлюзов.

Кроме того, разделение сетей должно основываться на ценности и классификации информации, хранимой или обрабатываемой в сети, уровнях доверия или сферах деятельности, для того чтобы снизить последствия от прерывания услуг.

Следует уделять внимание отделению беспроводных сетей от внутренних и частных сетей. Поскольку периметры беспроводных сетей не являются достаточно определенными, следует проводить оценку риска, чтобы идентифицировать меры и средства контроля и управления (например, строгую аутентификацию, криптографические методы и выбор частоты) для поддержки разделения сетей.

Сети все более распространяются за традиционные границы организации, поскольку создаются деловые партнерства, которые могут потребовать коммуникаций или совместного использования сетевой инфраструктуры и средств обработки информации. Такие расширения могут увеличить риск несанкционированного доступа к существующим информационным системам, которые используют сеть, причем в отношении некоторых из этих систем, вследствие их чувствительности или критичности

Управление сетевыми соединениями

Мера и средство контроля и управления

Присоединение пользователей к совместно используемым сетям, особенно тем, которые выходят за рамки организации, необходимо ограничивать в соответствии с политикой управления доступом и требованиями прикладных программ бизнеса.

Права пользователей в отношении сетевого доступа должны поддерживаться и обновляться в соответствии с требованиями политики управления доступом.

Возможность подсоединения пользователей может ограничиваться сетевыми шлюзами, фильтрующими трафик посредством предварительно определенных таблиц или правил.

Примерами прикладных программ, к которым следует применить ограничения являются:

a) обмен сообщениями, например электронная почта;

b) передача файлов;

c) интерактивный доступ;

d) доступ к прикладной программе.

Следует рассмотреть права доступа к сети, приуроченные к определенному времени суток или дате.

Требования политики управления доступом для совместно используемых сетей, особенно тех, которые выходят за рамки организации, могут вызвать необходимость внедрения дополнительных мер и средств контроля и управления, чтобы ограничить возможности пользователей по подсоединению.

Управление сетевой маршрутизацией

Мера и средство контроля и управления

Для сетей следует внедрять меры и средства контроля и управления маршрутизацией, чтобы обеспечить уверенность в том, что подсоединения компьютеров и информационные потоки не нарушают политику управления доступом к прикладным программам бизнеса.

Рекомендация по реализации

Необходимо, чтобы меры и средства контроля и управления маршрутизацией основывались на механизмах проверки реальных адресов источника и получателя.

Шлюзы безопасности могут использоваться для подтверждения адресов источника и получателя на внутренней и внешней точках управления сетью, если используются технологии трансляции сетевых адресов и (или) прокси-сервер. Необходимо, чтобы специалисты, занимающиеся внедрением, были осведомлены о преимуществах и недостатках различных используемых механизмов. Требования в отношении мер и средств контроля и управления маршрутизацией сети должны основываться на политике управления доступом.

Сети совместного использования, особенно те, которые выходят за рамки организации, могут потребовать внедрения дополнительных мер и средств контроля и управления маршрутизацией. Это, особенно, касается сетей, используемых совместно с пользователями третьей стороны (не организации).

5 Управление доступом к эксплуатируемой системе

Цель: Предотвратить несанкционированный доступ к эксплуатируемым системам.

Средства безопасности следует использовать, для того чтобы возможность осуществления доступа предоставлялась только авторизованным пользователям. Необходимо, чтобы данные средства могли обеспечить следующее:

a) аутентификацию авторизованных пользователей в соответствии с определенной политикой управления доступом;

b) b) регистрацию успешных и неудавшихся попыток аутентификации для осуществления доступа к системе;

c) c) регистрацию использования специальных системных привилегий;

d) d) срабатывание сигнализации при нарушении политик безопасности системы;

e) e) обеспечение соответствующих средств для аутентификации;

f) f) при необходимости, ограничение времени подсоединения пользователей.

Безопасные процедуры начала сеанса

Мера и средство контроля и управления

Доступ к эксплуатируемым системам должен контролироваться посредством безопасной процедуры начала сеанса.

Рекомендация по реализации

Процедура регистрации в эксплуатируемой системе должна быть спроектирована так, чтобы свести к минимуму возможность несанкционированного доступа. Поэтому необходимо, чтобы процедура начала сеанса раскрывала минимум информации о системе, во избежание оказания какой-либо ненужной помощи неавторизованному пользователю

Правильная процедура начала сеанса характеризуется следующими свойствами:

a) не отображает наименований системы или прикладных программ, пока процесс начала сеанса не будет успешно завершен;

b) отображает общее предупреждение о том, что доступ к компьютеру могут получить только авторизованные пользователи;

c) не предоставляет сообщений-подсказок в течение процедуры начала сеанса, которые могли бы помочь неавторизованному пользователю;

d) подтверждает информацию начала сеанса только по завершении ввода всех исходных данных, в случае ошибочного ввода, система не должна показывать, какая часть данных является правильной или неправильной;

e) ограничивает число разрешенных неудачных попыток начала сеанса (например три попытки) и предусматривает:

1) протоколирование неудачных и удачных попыток;

2) включение временной задержки прежде, чем будут разрешены дальнейшие попытки начала сеанса, или отклонение любых дальнейших попыток без специальной авторизации;

3) разъединение сеанса связи и передачи данных;

4) отправление предупредительного сообщения на системный пульт, если достигнуто максимальное число попыток начала сеанса;

5) установление числа повторного ввода паролей с учетом минимальной длины пароля и значимости защищаемой системы;

f) ограничивает максимальное и минимальное время, разрешенное для процедуры начала сеанса, если оно превышено, система должна прекратить начало сеанса;

g) отображает следующую информацию в отношении успешного завершения начала сеанса:

1) дату и время предыдущего успешного начала сеанса;

2) подробную информацию о любых неудачных попытках начала сеанса, начиная с последнего успешного начала сеанса;

h) не отображает введенный пароль или предусматривает скрытие знаков пароля с помощью символов;

i) не передает пароли открытым текстом по сети.

Дополнительная информация

Если пароли передаются в открытом виде по сети в течение начала сеанса сессии, они могут быть перехвачены в сети программой сетевого "сниффера".

Идентификация и аутентификация пользователя

Мера и средство контроля и управления

Необходимо, чтобы все пользователи имели уникальный идентификатор (идентификатор пользователя), предназначенный только для их личного использования, и должен быть выбран подходящий способ проверки для подтверждения заявленной подлинности пользователя.

Рекомендация по реализации

Меры и средства контроля и управления должна применяться в отношении всех типов пользователей (включая персонал технической поддержки, операторов, администраторов сети, системных программистов и администраторов баз данных).

Идентификаторы пользователей необходимо использовать для отслеживания действий подотчетного лица. Регулярные действия пользователей не должны выполняться из привилегированных учетных записей.

При исключительных обстоятельствах, когда имеется очевидная выгода для бизнеса, может использоваться общий идентификатор для группы пользователей или для выполнения определенной работы. В таких случаях необходимо документально оформлять разрешение руководства. Могут потребоваться дополнительные меры и средства контроля и управления для поддержания отслеживаемости.

Разрешение на индивидуальное использование группового идентификатора следует давать только тогда, когда функции общедоступны, или нет необходимости отслеживать действия, выполняемые с помощью данного идентификатора (например доступ только для чтения), или когда применяются другие меры контроля (например пароль для группового идентификатора выдается единовременно только для одного сотрудника и такой случай регистрируется).

Там, где требуются надежная аутентификация и идентификация личности, следует использовать аутентификационные методы, альтернативные по отношению к паролям, такие как криптографические средства, смарт-карты, токены или биометрические средства.

Пароли являются очень распространенным способом обеспечения идентификации и аутентификации, основанным на тайне, которую знает только пользователь. Того же результата можно достигнуть средствами криптографии и аутентификационными протоколами. Надежность идентификации и аутентификации пользователя должна соответствовать чувствительности информации, к которой нужно осуществлять доступ.

Такие объекты как токены с памятью или смарт-карты, которыми обладают пользователи, также могут применяться для идентификации и аутентификации. Биометрические технологии аутентификации, которые используют уникальные характеристики или особенности индивидуума, также могут служить для подтверждения подлинности личности. Сочетание различных технологий и механизмов, связанных безопасным способом, обеспечивает более надежную аутентификацию.

Система управления паролями

Мера и средство контроля и управления

Системы управления паролями должны быть интерактивными и должны обеспечивать уверенность в качестве паролей.

Система управления паролями должна:

a) предписывать использование индивидуальных пользовательских идентификаторов и паролей с целью установления персональной ответственности;

b) позволять пользователям выбирать и изменять свои пароли, и включать процедуру подтверждения ошибок ввода;

c) предписывать использование качественных паролей ;

d) принуждать к изменению паролей ;

e) заставлять пользователей изменять временные пароли при первом начале сеанса ;

f) вести учет предыдущих пользовательских паролей и предотвращать их повторное использование;

g) не отображать пароли на экране при их вводе;

h) хранить файлы паролей отдельно от данных прикладных систем;

i) хранить и передавать пароли в защищенной (например зашифрованной или хешированной) форме.

Пароли являются одним из главных средств подтверждения полномочий пользователя, осуществляющего доступ к сервисам компьютера.

Некоторые прикладные программы требуют, чтобы пользовательские пароли назначались независимым органом; в таких случаях перечисления b), d) и e) приведенных выше рекомендаций не применяются. В большинстве же случаев, пароли выбираются и поддерживаются пользователями

Использование системных утилит

Мера и средство контроля и управления

Использование утилит, которые могли бы обойти меры и средства контроля и управления эксплуатируемых систем и прикладных программ, следует ограничивать и строго контролировать.

Необходимо рассмотреть следующие рекомендации по использованию системных утилит:

a) использование процедур идентификации, аутентификации и авторизации для системных утилит;

b) отделение системных утилит от прикладных программ;

c) ограничение использования системных утилит минимальным числом доверенных авторизованных пользователей;

d) авторизация на использование специальных системных утилит;

e) ограничение доступности системных утилит, например на время внесения авторизованных изменений;

f) регистрация использования всех системных утилит;

g) определение и документальное оформление уровней авторизации в отношении системных утилит;

h) удаление или блокирование ненужного программного обеспечения утилит и системного программного обеспечения;

i) обеспечение недоступности системных утилит для пользователей, имеющих доступ к прикладным программам на системах, где требуется разделение обязанностей.

На большинстве компьютеров, как правило, установлена, одна или несколько системных обслуживающих программ (утилит), которые позволяют обойти меры и средства контроля и управления эксплуатируемых систем и прикладных программ.

Лимит времени сеанса связи

Мера и средство контроля и управления

Неактивные сеансы должны быть закрыты после определенного периода бездействия.

Рекомендация по реализации

Необходимо, чтобы механизм блокировки по времени обеспечивал очистку окна сеанса, а также, возможно позднее, после определенного периода бездействия закрывал прикладную программу и сетевые сеансы. Задержка, связанная с блокировкой по времени, должна отражать риски безопасности этой области, классификацию обрабатываемой информации и используемых прикладных программ, а также риски, связанные с пользователями оборудования.

Для некоторых систем может быть предусмотрена ограниченная форма средств блокировки по времени, которая очищает экран и предотвращает неавторизованный доступ, но не закрывает прикладные программы или сетевые сеансы.

Данная мера и средство контроля и управления особенно важна в местах повышенного риска, например в общедоступных местах или на внешней территории, находящейся вне сферы действия менеджмента безопасности организации. Для предотвращения доступа неавторизованных лиц и атак типа "отказ в обслуживании" сеансы необходимо закрывать.

Ограничения времени соединения

Мера и средство контроля и управления

Ограничения на время соединения должны быть использованы для обеспечения дополнительной безопасности прикладных программ с высокой степенью риска.

Рекомендация по реализации

Необходимо рассмотреть меры и средства контроля и управления в отношении времени подсоединения для чувствительных компьютерных приложений, особенно в местах повышенного риска, например общедоступных местах или на внешней территории, находящейся вне сферы действия менеджмента безопасности организации.

Примерами таких ограничений являются:

a) использование заранее определенных отрезков времени, например для пакетной передачи файлов или регулярных интерактивных сеансов небольшой продолжительности;

b) ограничение времени подключения нормальными часами работы организации, если нет необходимости в сверхурочной или более продолжительной работе;

c) проведение повторной аутентификации через запланированные интервалы времени.

Ограничение периода, в течение которого разрешены подсоединения к компьютерным сервисам, уменьшает интервал времени, в течение которого существует риск неавторизованного доступа. Ограничение продолжительности активных сеансов не позволяет пользователям держать сеансы открытыми, чтобы предотвратить повторную аутентификацию.

6 Управление доступом к информации и прикладным программам

Цель: Предотвратить неавторизованный доступ к информации прикладных систем. Необходимо использовать средства безопасности для ограничения доступа к прикладным системам и внутри данных систем.

Круг лиц, имеющих логический доступ к прикладному программному обеспечению и информации, должен быть ограничен только авторизованными пользователями. Необходимо, чтобы прикладные системы обеспечивали следующее:

a) управление доступом пользователей к информации и функциям прикладных систем в соответствии с определенной политикой управления доступом;

b) защиту от неавторизованного доступа любой утилиты, программного обеспечения эксплуатируемой системы и вредоносной программы, которые позволяют отменять или обходить меры и средства контроля и управления системы или прикладных программ;

c) c) не представляли угрозу безопасности другим системам, совместно с которыми используются информационные ресурсы.

Ограничение доступа к информации

Мера и средство контроля и управления

Доступ пользователей и персонала поддержки к информации и функциям прикладных систем должен ограничиваться в соответствии с определенной политикой в отношении управления доступом.

Рекомендация по реализации

Ограничения доступа должны основываться на требованиях в отношении отдельных прикладных программ бизнеса. Политика управления доступом должна соответствовать политике доступа организации.

Необходимо рассмотреть возможность применения следующих рекомендаций для соблюдения требований по ограничению доступа:

a) наличие пунктов меню, позволяющих управлять доступом к функциям прикладных систем;

b) управление правами доступа пользователей, например чтение, запись, удаление, выполнение;

c) управление правами доступа других прикладных программ;

d) обеспечение уверенности в том, что данные, выводимые из прикладных систем, обрабатывающих чувствительную информацию, содержат только требуемую информацию и отправлены только в адреса авторизованных терминалов и мест назначения; необходим периодический анализ процесса вывода для обеспечения уверенности в том, что избыточная информация удалена.

Изоляция чувствительных систем

Мера и средство контроля и управления

Чувствительные системы должны иметь специализированную (изолированную) вычислительную среду.

Рекомендация по реализации

В отношении систем, обрабатывающих чувствительную информацию, необходимо рассмотреть следующее:

a) владелец прикладной программы должен определить и документально оформить степень чувствительности данной прикладной программы ;

b) если чувствительная прикладная программа должна работать в среде совместного использования, владельцем данной прикладной программы должны быть выявлены другие прикладные программы, с которыми будут совместно использоваться ресурсы, а также идентифицированы и приняты соответствующие риски.

Некоторые прикладные программы системы достаточно чувствительны к потенциальному ущербу и поэтому требуют особой эксплуатации. Чувствительность может указывать, что прикладная программа система:

a) должна работать на выделенном компьютере;

b) должна разделять ресурсы только с доверенными прикладными программами системы.

Изоляция может быть достигнута при использовании физических или логических методов.

7 Мобильная вычислительная техника и дистанционная работа

Цель: Обеспечить уверенность в информационной безопасности при использовании средств мобильной вычислительной техники и дистанционной работы

Следует соизмерять требуемую защиту со специфичными рисками работы в удаленном режиме. При использовании мобильной вычислительной техники следует учитывать риски, связанные с работой в незащищенной среде, и применять соответствующие средства защиты. В случаях дистанционной работы организации следует предусмотреть защиту мест дистанционной работы и обеспечить уверенность в соответствующей организации подобного способа работы.

Мобильная вычислительная техника и связь

Мера и средство контроля и управления

Необходимо принять формальную политику и обеспечить соответствующие меры безопасности для защиты от рисков, связанных с работой со средствами мобильной вычислительной техники и связи.

Рекомендация по реализации

При использовании мобильных вычислительных средств и средств связи, например ноутбуков, карманных компьютеров, лэптопов, смарт-карт и мобильных телефонов, необходимо принимать специальные меры для обеспечения уверенности в том, что бизнес-информация не скомпрометирована. Политика использования мобильных вычислительных средств должна учитывать риски, связанные с работой с переносными устройствами в незащищенной среде.

Политика использования мобильных вычислительных средств должна включать требования к физической защите, управлению доступом, использованию средств криптографии, резервирования и защиты от вирусов. Такая политика должна также включать правила и рекомендации относительно подсоединения мобильных средств к сетям, а также руководство по использованию этих средств в общедоступных местах.

Следует проявлять осторожность при использовании мобильных вычислительных средств в общедоступных местах, конференц-залах и других незащищенных местах вне организации. Необходимо обеспечить защиту от неавторизованного доступа или раскрытия информации, хранимой и обрабатываемой этими средствами, например с помощью средств криптографии .

Важно при использовании мобильных вычислительных средств в общедоступных местах проявлять осторожность, во избежание риска вмешательства неавторизованных лиц. Необходимо внедрить и поддерживать в актуальном состоянии процедуры защиты от вредоносной программы .

Необходимо регулярно делать резервные копии критической информации бизнеса. Следует также обеспечить доступность оборудования для быстрого и удобного резервного копирования информации. В отношении резервных копий необходимо обеспечить адекватную защиту, например от кражи или потери информации.

Соответствующую защиту необходимо обеспечить в отношении использования мобильных средств, подсоединенных к сетям. Удаленный доступ к информации бизнеса через общедоступную сеть с использованием мобильных средств вычислительной техники следует осуществлять только после успешной идентификации и аутентификации, а также при условии внедрения соответствующих механизмов управления доступом (см. 11.4).

Мобильные вычислительные средства необходимо также физически защищать от краж, особенно когда их оставляют без присмотра/забывают, например в автомобилях или других видах транспорта, гостиничных номерах, конференц-центрах и местах встреч. Для случаев потери или кражи мобильных вычислительных средств должна быть установлена специальная процедура, учитывающая законодательные, страховые и другие требования безопасности организации. Оборудование, в котором переносится важная, чувствительная и (или) критическая информация бизнеса, не следует оставлять без присмотра и по возможности должно быть физически заблокировано или должны быть использованы специальные замки для обеспечения безопасности оборудования (см. 9.2.5).

Необходимо провести тренинг сотрудников, использующих мобильные вычислительные средства, с целью повышения осведомленности о дополнительных рисках, связанных с таким способом работы и мерах и средствах контроля и управления, которые должны быть выполнены.

Беспроводные подсоединения к сети мобильной связи аналогичны другим типам подсоединения к сети, однако они имеют важные отличия, которые необходимо учитывать при определении мер и средств контроля и управления. Типичными отличиями являются:

a) некоторые беспроводные небезупречные протоколы безопасности;

b) невозможность резервного копирования информации в мобильных вычислительных средствах вследствие ограниченной пропускной способности сети и (или) из-за того, что переносное оборудование не может быть подсоединено на время, которое запланировано для резервирования.

Дистанционная работа

Мера и средство контроля и управления

Политика, планы и процедуры эксплуатации должны быть разработаны и внедрены для дистанционной работы.

Рекомендация по реализации

Организации должны разрешать дистанционную работу только при уверенности в том, что применяются соответствующие соглашения о безопасности и меры и средства контроля и управления, которые, в свою очередь, согласуются с политикой безопасности организации.

Следует обеспечить необходимую защиту места дистанционной работы в отношении, например хищения оборудования и информации, несанкционированного раскрытия информации, несанкционированного удаленного доступа к внутренним системам организации или неправильного использования оборудования. Дистанционная работа должна быть санкционирована и контролируема руководством, и должна быть обеспечена уверенность в том, что имеются соответствующие меры для данного способа работы.

Необходимо принимать во внимание следующее:

a) существующую физическую безопасность места дистанционной работы, включая физическую безопасность здания и окружающей среды;

b) предлагаемые условия дистанционной работы;

c) требования в отношении безопасности коммуникаций, учитывая потребность в удаленном доступе к внутренним системам организации, чувствительность информации, к которой будет осуществляться доступ и которая будет передаваться по каналам связи, а также чувствительность самих внутренних систем;

d) угрозу несанкционированного доступа к информации или ресурсам со стороны других лиц, использующих место дистанционной работы, например членов семьи и друзей;

e) использование домашних компьютерных сетей, а также требования или ограничения в отношении конфигурации услуг беспроводных сетей;

f) политики и процедуры для предотвращения споров, касающихся прав на интеллектуальную собственность, разработанную на оборудовании, находящемся в частной собственности;

g) доступ к оборудованию, находящемуся в частной собственности (для проверки безопасности машины или во время проведения расследований), который может быть запрещен законодательством;

h) лицензионные соглашения в отношении программного обеспечения, которые таковы, что организация может стать ответственной за лицензирование клиентского программного обеспечения на рабочих станциях, находящихся в частной собственности сотрудников, подрядчиков или пользователей третьей стороны;

i) требования в отношении антивирусной защиты и межсетевых экранов.

Рекомендации и необходимые организационные меры включают, в частности:

a) обеспечение подходящим оборудованием и мебелью для дистанционной работы в тех случаях, когда запрещается использование оборудования, находящегося в частной собственности, если оно не находится под контролем организации;

b) определение видов разрешенной работы, времени работы, классификацию информации, которая может поддерживаться внутренними системами и услугами, к которым разрешен доступ сотруднику в дистанционном режиме;

c) обеспечение подходящим телекоммуникационным оборудованием, включая методы обеспечения безопасности удаленного доступа;

d) физическую безопасность;

e) правила и рекомендации в отношении доступа членов семьи и друзей к оборудованию и информации;

f) обеспечение технической поддержки и обслуживания аппаратного и программного обеспечения;

g) обеспечение страхования;

h) процедуры в отношении резервного копирования данных и обеспечения непрерывности бизнеса;

i) аудит и мониторинг безопасности;

j) аннулирование полномочий, отмену прав доступа и возвращение оборудования в случае прекращения работы в дистанционном режиме.

При работе в дистанционном режиме применяются коммуникационные технологии, дающие возможность сотрудникам работать в конкретном удаленном месте за пределами своей организации.