Тема: Безопасность, связанная с персоналом. Физическая безопасность и защита от воздействий окружающей среды

1 вопрос: Безопасность, связанная с персоналом

Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и представители третьей стороны осознают свои обязанности и способны выполнять предусмотренные для них роли, и снизить риск хищения, мошенничества или нецелевого использования средств обработки информации. Обязанности, связанные с обеспечением безопасности, следует оговаривать перед трудоустройством в соответствующих должностных инструкциях и условиями работы. Необходима соответствующая проверка всех кандидатов на должность, подрядчиков и представителей третьей стороны, особенно если работа связана с секретностью. Сотрудники, подрядчики и представители третьей стороны, использующие средства обработки информации организации, должны подписывать соглашение в отношении их ролей и обязанностей в области безопасности.

Роли и обязанности в области безопасности сотрудников, подрядчиков и представителей третьей стороны необходимо определять и оформлять документально в соответствии с политикой информационной безопасности организации.

Роли и обязанности в области безопасности должны включать в себя требования в отношении:

a) реализации и действия в соответствии с политиками информационной безопасности организации ;

b) защиты активов от несанкционированного доступа, разглашения сведений, модификации, разрушений или вмешательства;

c) выполнения определенных процессов или деятельности, связанных с безопасностью;

d) обеспечения уверенности в том, что на индивидуума возлагается ответственность за предпринимаемые действия;

e) информирования о событиях или потенциальных событиях, связанных с безопасностью, или других рисках безопасности для организации.

Роли и обязанности в области безопасности должны быть определены и доведены до претендентов на работу до их трудоустройства.

Для документального оформления ролей и обязанностей в области безопасности могут использоваться должностные инструкции. Роли и обязанности в области безопасности лиц, поступивших на работу не через процесс трудоустройства, принятый в организации, а, например с помощью сторонней организации, должны быть также четко определены и доведены до сведения.

Предварительная проверка

Тщательная проверка всех кандидатов на постоянную работу, подрядчиков и представителей третьей стороны должна проводиться согласно соответствующим законам, инструкциям и правилам этики, пропорционально требованиям бизнеса, классификации информации, к которой будет осуществляться доступ, и предполагаемым рискам.

При проверке следует учитывать конфиденциальность, защиту персональных данных и (или) трудовое законодательство. Такая проверка должна включать следующие элементы:

a) наличие положительных рекомендаций, в частности, в отношении деловых и личных качеств претендента;

b) проверку (на предмет полноты и точности) биографии претендента;

c) подтверждение заявленного образования и профессиональной квалификации;

d) независимую проверку подлинности документов, удостоверяющих личность (паспорта или заменяющего его документа);

e) более детальную проверку, например кредитоспособности или на наличие судимости.

В случаях, когда новому сотруднику непосредственно после приема на работу или в дальнейшем предоставляется доступ к средствам обработки информации, в частности, обрабатывающим чувствительную информацию, например финансовую или секретную информацию, организации следует проводить дополнительную, более детальную проверку.

Процедуры должны определять критерии и ограничения процесса проверки, например кто имеет право проводить проверку сотрудников, каким образом, когда и с какой целью проводится эта проверка.

Предварительную проверку также следует проводить для подрядчиков и представителей третьей стороны. В тех случаях, когда подрядчики предоставляются через кадровое агентство, контракт с агентством должен четко определять обязанности агентства по предварительной проверке претендентов и процедурам уведомления, которым оно должно следовать, если предварительная проверка не была закончена, или если ее результаты дают основания для сомнения. Как бы то ни было, в договорах с третьей стороной должны четко определяться все обязанности и процедуры уведомления, необходимые для предварительной проверки.

Информацию обо всех рассматриваемых кандидатах, претендующих на занятие должностей в организации, следует собирать и обрабатывать согласно законодательству, действующему в соответствующей юрисдикции. В зависимости от действующего законодательства, данные кандидаты должны быть предварительно проинформированы о деятельности, связанной с предварительной проверкой.

Условия занятости

В рамках своих договорных обязательств, сотрудники, подрядчики и представители третьей стороны должны согласовать и подписать условия своего трудового договора, устанавливающего их ответственность и ответственность организации в отношении информационной безопасности.

Условия занятости должны отражать политику безопасности организации и кроме того разъяснять и констатировать:

a) что все сотрудники, подрядчики и представители третьей стороны, имеющие доступ к чувствительной информации, должны подписывать соглашение о конфиденциальности или неразглашении прежде, чем им будет предоставлен доступ к средствам обработки информации;

b) правовую ответственность и права сотрудников, подрядчиков и любых других клиентов, например в части законов об авторском праве или законодательства о защите персональных данных;

c) обязанности в отношении классификации информации и менеджмента активов организации, связанных с информационными системами и услугами, выполняются сотрудником, подрядчиком или представителем третьей стороны;

d) ответственность сотрудника, подрядчика или представителя третьей стороны за обработку информации, получаемой от других фирм и сторонних организаций;

e) ответственность организации за обработку персональной информации, включая персональную информацию, полученную в результате или в процессе работы в организации;

f) ответственность, распространяющуюся также и на работу вне помещений организации и в нерабочее время, например в случае исполнения работы на дому;

g) действия, которые должны быть предприняты в случае, если сотрудник, подрядчик или представитель третьей стороны игнорирует требования безопасности организации.

Организация должна обеспечивать уверенность в том, что сотрудники, подрядчики и представители третьей стороны согласны с условиями, касающимися информационной безопасности и соответствующими типу и объему доступа, который они будут иметь к активам организации, связанным с информационными системами и услугами.

При необходимости ответственность, возлагаемая на сотрудника по условиям занятости, должна сохраняться сотрудником в течение определенного периода времени и после окончания работы в организации.

Может быть использован кодекс поведения для распространения информации, касающейся обязанностей сотрудников, подрядчиков или представителей третьей стороны в отношении конфиденциальности, защиты информации, правил этики, соответствующего использования оборудования и средств организации, а также порядка деятельности. Подрядчик или представители третьей стороны могут быть связаны со сторонней организацией, с которой, в свою очередь, может потребоваться заключить договорные соглашения от имени лица, подписавшего договор.

В течение занятости

Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и представители третьей стороны осведомлены об угрозах и проблемах, связанных с информационной безопасностью, о мере их ответственности и обязательствах, а также оснащены всем необходимым для поддержки политики безопасности организации, что снижает риск человеческого фактора. Следует определять обязанности руководства, чтобы обеспечить уверенность в том, что безопасность обеспечивается на протяжении всего времени занятости сотрудника в организации. Адекватный уровень осведомленности, обучения и тренинг процедурам безопасности и правильному использованию средств обработки информации должен быть обеспечен всем сотрудникам, подрядчикам и представителям третьей стороны, чтобы свести к минимуму возможные риски безопасности. Должен быть установлен формальный дисциплинарный процесс для рассмотрения нарушений безопасности.

Обязанности руководства

Руководство организации должно требовать, чтобы сотрудники, подрядчики и представители третьей стороны обеспечивали безопасность в соответствии с установленными политиками и процедурами организации.

Руководство обязано обеспечить уверенность в том, что сотрудники, подрядчики и представители третьей стороны:

a) были проинформированы о своих ролях и обязанностях в области информационной безопасности прежде, чем им был предоставлен доступ к чувствительной информации или информационным системам;

b) обеспечены рекомендациями по формулированию их предполагаемых ролей в отношении безопасности в рамках организации;

c) заинтересованы следовать политикам безопасности организации;

d) достигают уровня осведомленности в отношении безопасности, соответствующего их ролям и обязанностям в организации;

e) следуют условиям занятости, которые включают политику информационной безопасности организации и соответствующие методы работы;

f) продолжают поддерживать соответствующие навыки и квалификацию

Если сотрудники, подрядчики и представители третьей стороны не были осведомлены о своих обязанностях в отношении безопасности, они могут причинить значительный ущерб организации. Заинтересованный персонал, вероятно, будет более надежным и вызовет меньше инцидентов информационной безопасности.

Неэффективный менеджмент может являться причиной того, что персонал будет чувствовать себя недооцененным, что в дальнейшем может иметь негативные последствия для организации. Например неэффективный менеджмент может привести к игнорированию безопасности или возможному нецелевому использованию активов организации.

Осведомленность, обучение и тренинг в области информационной безопасности

Все сотрудники организации и, где необходимо, подрядчики и представители третьей стороны, должны пройти соответствующее обучение и получать на регулярной основе обновленные варианты политик и процедур, принятых в организации и необходимых для выполнения их рабочих функций.

Обучение, обеспечивающее осведомленность, следует начинать с формального вводного процесса, предназначенного для ознакомления с политиками и ожиданиями организации в области безопасности прежде, чем будет предоставлен доступ к информации или услугам.

Постоянное обучение должно охватывать требования безопасности, правовую ответственность, управление бизнесом, а также обучение правильному использованию средств обработки информации, например процедуре начала сеанса, использованию пакетов программ и информации о дисциплинарном процессе.

Деятельность, связанная с обеспечением осведомленности, обучения и тренинга в отношении безопасности должна быть адекватной и соответствовать роли, обязанностям и квалификации лица, и должна включать информацию об известных угрозах, о контактном лице для получения дополнительной консультации по безопасности, а также о соответствующих каналах для сообщения об инцидентах информационной безопасности.

Обучение с целью повышения осведомленности направлено на то, чтобы дать возможность отдельным лицам распознавать проблемы и инциденты информационной безопасности, и реагировать в соответствии с потребностями их рабочей функции.

Дисциплинарный процесс

Должен существовать формальный дисциплинарный процесс, применяемый в отношении сотрудников, совершивших нарушение безопасности. Не следует начинать дисциплинарный процесс, не получив предварительного подтверждения того, что нарушение безопасности произошло.

Формальный дисциплинарный процесс призван обеспечить уверенность в корректном и справедливом рассмотрении дел сотрудников, подозреваемых в совершении нарушений безопасности. Формальный дисциплинарный процесс следует обеспечивать для дифференцированного реагирования, учитывающего такие факторы, как тип и тяжесть нарушения и его негативное влияние на бизнес, совершено ли нарушение впервые или повторно, получил ли нарушитель должную подготовку, соответствующее законодательство, договоры в сфере бизнеса и другие факторы, если в этом есть необходимость. В серьезных случаях неправомерного поведения процесс должен обеспечивать возможность безотлагательного аннулирования обязанностей, прав доступа и привилегий сотрудника и, при необходимости, немедленного удаления его из информационного процесса.

Дисциплинарный процесс следует также использовать как сдерживающее средство для предотвращения совершения сотрудниками, подрядчиками и представителями третьей стороны нарушений политик и процедур безопасности, принятых в организации, и каких-либо других нарушений безопасности.

Прекращение или смена занятости

Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и представители третьей стороны покидают организацию или меняют занятость должным образом Администрация обязана обеспечить уверенность в том, что при увольнении сотрудников, подрядчиков и представителей третьей стороны из организации, осуществляется возврат всего оборудования, а также выполняется аннулирование всех прав доступа. Обязанности в отношении прекращения занятости или смены занятости должны быть четко определены и установлены.

Информирование о прекращении обязанностей должно включать в себя актуальные требования безопасности и правовую ответственность, и, при необходимости, обязанности, содержащиеся в соглашении о конфиденциальности, а также условия занятости, продолжающие действовать в течение определенного периода времени после прекращения занятости сотрудников, подрядчиков или представителей третьей стороны. Ответственность и служебные обязанности, продолжающие оставаться действительными после прекращения занятости, должны содержаться в договорах с сотрудниками, подрядчиками или представителями третьей стороны.

Отдел кадров, как правило, отвечает за общий процесс прекращения занятости и действует совместно с руководителем увольняемого лица, чтобы обеспечить управление аспектами безопасности значимых процедур. В отношении подрядчика данный процесс может быть осуществлен агентством, несущим ответственность за подрядчика, а в отношении представителя третьей стороны - его организацией.

Сотрудников, клиентов, подрядчиков или представителей третьей стороны необходимо информировать об изменениях кадрового состава и действующих договоренностей.

Возврат активов

Все сотрудники, подрядчики и представители третьей стороны обязаны вернуть организации все активы, находящиеся в их пользовании, при прекращении их занятости, договора или соглашения. Процесс прекращения занятости должен быть формализован таким образом, чтобы включать в себя возврат всего ранее выданного программного обеспечения, корпоративных документов и оборудования. Необходимо возвращать также другие активы организации, например мобильную вычислительную технику, кредитные карты, карты доступа, программное обеспечение, руководства и информацию, хранящуюся на электронных носителях.

В тех случаях, когда сотрудник, подрядчик или представитель третьей стороны покупает оборудование организации или использует свое собственное оборудование, необходимо следовать процедурам, обеспечивающим уверенность в том, что вся значимая информация была передана организации и удалена из оборудования безопасным образом.

В случаях, когда сотрудник, подрядчик или представитель третьей стороны располагает знаниями, важными для продолжающихся работ, такую информацию следует оформлять документально и передавать организации.

Аннулирование прав доступа

Права доступа всех служащих, подрядчиков и представителей третьей стороны к информации и средствам обработки информации должны быть аннулированы при прекращении занятости, договора или соглашения, или скорректированы при смене занятости.

При прекращении занятости, права доступа к активам, связанным с информационными системами, и услугам необходимо пересматривать. Это позволит определять, нужно ли аннулировать права доступа. Смена занятости должна сопровождаться аннулированием всех прав доступа, которые не санкционированы для новой занятости. Права доступа, которые должны быть аннулированы или адаптированы, касаются физического и логического доступа, ключей, идентификационных карт, средств обработки информации, подписок и удаления из любой документации, в которой они идентифицируются как фактические сотрудники организации. Если увольняемый сотрудник, подрядчик или представитель третьей стороны знал пароли к учетным записям, остающимся активными, то эти пароли должны быть изменены после прекращения занятости, договора или соглашения, или при смене занятости.

Права доступа к информационным активам и средствам обработки информации следует уменьшать или аннулировать до прекращения занятости или смены места занятости, в зависимости от оценки факторов риска, например:

a) было ли прекращение занятости или смена места занятости инициированы сотрудником, подрядчиком или представителем третьей стороны, или руководством, и причина прекращения занятости;

b) текущие обязанности сотрудника, подрядчика или любого другого представителя;

c) значимость активов, доступных в настоящий момент.

При определенных обстоятельствах права доступа могут распределяться на основе доступности для большего количества людей, чем только для увольняемого сотрудника, подрядчика или представителя третьей стороны, например групповые идентификаторы. При таких обстоятельствах увольняемых лиц следует исключать из любых списков группового доступа, и следует предпринимать меры, рекомендующие всем другим связанным с доступом сотрудникам, подрядчикам и представителям третьей стороны не осуществлять совместно с увольняемым лицом использования этой информации.

В случаях, когда прекращение занятости инициируется руководством, рассерженные сотрудники, подрядчики или представители третьей стороны могут преднамеренно разрушать информацию или повреждать средства обработки информации. В случаях ухода в отставку, некоторые лица склонны собирать информацию для будущего использования.

2 вопрос: Физическая безопасность и защита от воздействий окружающей среды

Цель: Предотвращать неавторизованный физический доступ, повреждение и воздействие в отношении помещений и информации организации. Средства обработки критической или чувствительной информации необходимо размещать в зонах безопасности, обозначенных определенным периметром безопасности, обладающим соответствующими защитными барьерами и средствами, контролирующими вход. Эти зоны должны быть физически защищены от неавторизованного доступа, повреждения и воздействия. Уровень защищенности должен быть соразмерен выявленным рискам.

Для защиты зон, которые содержат информацию и средства обработки информации, следует использовать периметры безопасности (барьеры, например стены, управляемые картами доступа ворота или турникеты, управляемые человеком).

В отношении физических периметров безопасности рекомендуется рассматривать и реализовывать, при необходимости, следующие рекомендации:

a) периметры безопасности должны быть четко определены, а размещение и надежность каждого из периметров должны зависеть от требований безопасности активов, находящихся в пределах периметра, и от результатов оценки риска;

b) периметры здания или помещений, где расположены средства обработки информации, должны быть физически прочными (т.е. не должно быть никаких промежутков в периметре или мест, через которые можно было бы легко проникнуть); внешние стены помещений должны иметь твердую конструкцию, а все внешние двери должны быть соответствующим образом защищены от неавторизованного доступа, например оснащены шлагбаумом, сигнализацией, замками т.п.; двери и окна помещений в отсутствие сотрудников должны быть заперты, и внешняя защита должна быть предусмотрена для окон, особенно если они находятся на уровне земли;

c) должна быть выделена и укомплектована персоналом зона регистрации посетителей, или должны существовать другие меры для контроля физического доступа в помещения или здания; доступ в помещения и здания должен предоставляться только авторизованному персоналу;

d) где необходимо, должны быть построены физические барьеры, предотвращающие неавторизованный физический доступ и загрязнение окружающей среды;

e) все аварийные выходы на случай пожара в периметре безопасности должны быть оборудованы аварийной сигнализацией, должны подвергаться мониторингу и тестированию вместе со стенами, чтобы создать требуемый уровень устойчивости в соответствии с применимыми региональными, национальными и международными стандартами; они должны эксплуатироваться в соответствии с местной системой противопожарных правил безотказным образом;

f) следует устанавливать необходимые системы обнаружения вторжения, соответствующие национальным, региональным или международным стандартам, и регулярно тестировать их на предмет охвата всех внешних дверей и доступных окон, свободные помещения необходимо ставить на сигнализацию; аналогично следует оборудовать и другие зоны, например серверную комнату или помещение, где расположены средства коммуникаций;

g) необходимо физически изолировать средства обработки информации, контролируемые организацией, от средств, контролируемых сторонними организациями.

Физическая защита может быть обеспечена созданием одного или нескольких физических барьеров вокруг помещений и средств обработки информации организации. Использование нескольких барьеров дает дополнительную защиту, и повреждение одного барьера не означает немедленного нарушения безопасности.

Зоной безопасности может быть запираемый офис или несколько помещений внутри физического барьера безопасности. Между зонами с различными требованиями безопасности, находящимися внутри периметра безопасности, могут потребоваться дополнительные барьеры и периметры для контроля физического доступа.

В отношении безопасности физического доступа особое внимание следует обращать на здания, в которых размещено несколько организаций.

Меры и средства контроля и управления физическим входом

Зоны безопасности необходимо защищать с помощью соответствующих мер и средств контроля и управления входа, чтобы обеспечить уверенность в том, что доступ разрешен только авторизованному персоналу.

Следует принимать во внимание следующие рекомендации:

a) дату и время входа и выхода посетителей следует регистрировать, и всех посетителей необходимо сопровождать, или они должны обладать соответствующим допуском; доступ следует предоставлять только для выполнения определенных авторизованных задач, а также необходимо инструктировать посетителей на предмет требований безопасности, и действий в случае аварийных ситуаций;

b) доступ к зонам, где обрабатывается или хранится чувствительная информация, должен контролироваться и предоставляться только авторизованным лицам; следует использовать средства аутентификации, например контрольную карту доступа с персональным идентификационным номером (ПИН) для авторизации и проверки всех видов доступа; необходимо вести защищенные контрольные записи регистрации доступа;

c) необходимо требовать, чтобы все сотрудники, подрядчики и представители третьей стороны носили ту или иную форму видимого идентификатора и незамедлительно уведомляли сотрудников службы безопасности о замеченных несопровождаемых посетителях и лицах, не носящих видимого идентификатора;

d) доступ в зоны безопасности или к средствам обработки чувствительной информации персоналу вспомогательных служб третьей стороны следует предоставлять только при необходимости; такой доступ должен быть санкционирован и сопровождаться соответствующим контролем;

e) права доступа в зоны безопасности следует регулярно анализировать, пересматривать, и аннулировать при необходимости

Безопасность зданий, производственных помещений и оборудования

Необходимо разработать и реализовать физическую защиту зданий, производственных помещений и оборудования.

В отношении защиты зданий, производственных помещений и оборудования необходимо учитывать следующие рекомендации:

a) следует принимать в расчет соответствующие правила и стандарты, касающиеся охраны здоровья и безопасности труда;

b) основное оборудование должно быть расположено в местах, где ограничен доступ посторонним лицам;

c) здания, где это применимо, должны давать минимальную информацию относительно их предназначения, не должны иметь явных признаков снаружи или внутри здания, позволяющих установить наличие деятельности по обработке информации;

d) справочники и внутренние телефонные книги, указывающие на местоположение средств обработки чувствительной информации, не должны быть легкодоступными для посторонних лиц.

Защита от внешних угроз и угроз со стороны окружающей среды

Необходимо разработать и реализовать физическую защиту от нанесения ущерба, который может явиться результатом пожара, наводнения, землетрясения, взрыва, общественных беспорядков и других форм природных или антропогенных бедствий.

Необходимо предусмотреть любые угрозы безопасности, исходящие от соседних помещений, например пожар в соседнем здании, воду, текущую с крыши или затопившую этажи, находящиеся ниже уровня земли, или взрыв на улице.

Для предотвращения ущерба от пожара, наводнения, землетрясения, взрыва, общественных беспорядков и других форм природных или антропогенных бедствий, следует учитывать следующие рекомендации:

a) обеспечить надежное хранение опасных или горючих материалов на достаточном расстоянии от охраняемой зоны; большие запасы, например бумаги для печатающих устройств, не следует хранить в пределах зоны безопасности;

b) резервное оборудование и носители данных следует размещать на безопасном расстоянии во избежание повреждения от последствия стихийного бедствия в основном здании;

c) следует обеспечить и соответствующим образом разместить необходимые средства пожаротушения.

Работа в зонах безопасности

Необходимо разработать и реализовать физическую защиту и рекомендации по работе в зонах безопасности

Необходимо рассмотреть следующие рекомендации:

a) о существовании зоны безопасности и проводимых там работах персонал должен быть осведомлен по "принципу необходимого знания";

b) из соображений безопасности и предотвращения возможности злонамеренных действий в зонах безопасности необходимо избегать выполнения работы без надлежащего контроля со стороны уполномоченного персонала;

c) должна быть обеспечена безопасность внешних дверей зоны приемки и отгрузки в то время, когда внутренние двери открыты;

d) поступающие материальные ценности должны быть проверены на предмет потенциальных угроз прежде, чем они будут перемещены из зоны приемки и отгрузки к месту использования;

e) при поступлении материальные ценности должны регистрироваться в соответствии с процедурами менеджмента активов;

f) там, где возможно, ввозимые и вывозимые грузы должны быть физически разделены.

Зоны общего доступа, приемки и отгрузки

Места доступа, например зоны приемки и отгрузки, и другие места, где неавторизованные лица могут проникнуть в помещения, должны находиться под контролем и, по возможности, должны быть изолированы от средств обработки информации, во избежание неавторизованного доступа.

Необходимо рассмотреть следующие рекомендации:

a) доступ к зоне приемки и отгрузки с внешней стороны здания должен быть разрешен только определенному и авторизованному персоналу;

b) зона приемки и отгрузки должна быть организована так, чтобы поступающие материальные ценности могли быть разгружены без предоставления персоналу поставщика доступа к другим частям здания;

c) должна быть обеспечена безопасность внешних дверей зоны приемки и отгрузки в то время, когда внутренние двери открыты;

d) поступающие материальные ценности должны быть проверены на предмет потенциальных угроз прежде, чем они будут перемещены из зоны приемки и отгрузки к месту использования;

e) при поступлении материальные ценности должны регистрироваться в соответствии с процедурами менеджмента активов;

Безопасность оборудования

Цель: Предотвращать потерю, повреждение, кражу или компрометацию активов и прерывание деятельности организации

Оборудование необходимо защищать от физических угроз и воздействия окружающей среды

Обеспечение безопасности оборудования (включая используемое вне организации и выносимое имущество) необходимо для уменьшения риска неавторизованного доступа к информации и защиты ее от потери или повреждения. При этом следует учесть размещение и утилизацию оборудования. Могут потребоваться специальные меры и средства контроля и управления для защиты от физических угроз, а также для защиты инфраструктуры поддерживающих услуг, например системы электропитания и кабельной разводки.

Размещение и защита оборудования

Оборудование должно быть размещено и защищено так, чтобы уменьшить риски от угроз окружающей среды и возможности неавторизованного доступа. Необходимо рассмотреть следующие рекомендации по защите оборудования:

a) оборудование следует размещать таким образом, чтобы свести к минимуму излишний доступ в рабочие зоны;

b) средства обработки информации, обрабатывающие чувствительные данные, следует размещать и ограничивать угол обзора таким образом, чтобы уменьшить риск просмотра информации неавторизованными лицами во время их использования, а средства хранения информации следует защищать от неавторизованного доступа;

c) отдельные элементы оборудования, требующие специальной защиты, следует изолировать для снижения общего уровня требуемой защиты;

d) меры и средства контроля и управления должны быть внедрены таким образом, чтобы свести к минимуму риск потенциальных физических угроз (воровство, пожар, взрывы, задымление, затопление или неисправность водоснабжения, пыль, вибрация, химическое воздействие, помехи в электроснабжении, помехи в работе линий связи, электромагнитное излучение и вандализм);

e) необходимо устанавливать правила в отношении приема пищи, питья и курения вблизи средств обработки информации;

f) следует проводить мониторинг состояния окружающей среды по выявлению условий, например температуры и влажности, которые могли бы оказать неблагоприятное влияние на функционирование средств обработки информации;

g) на всех зданиях должна быть установлена защита от молнии, а фильтры защиты от молнии должны быть установлены на входе всех линий электропередачи и линий коммуникации;

h) в отношении оборудования, расположенного в промышленной среде, следует использовать специальные средства защиты, например защитные пленки для клавиатуры;

i) оборудование, обрабатывающее чувствительную информацию, должно быть защищено, чтобы свести к минимуму риск утечки информации вследствие излучения.

Поддерживающие услуги

Оборудование необходимо защищать от перебоев подачи электроэнергии и других сбоев, связанных с перебоями в обеспечении поддерживающих услуг.

Все поддерживающие услуги, например электроснабжение, водоснабжение, канализация, отопление/вентиляция и кондиционирование воздуха, должны быть адекватными для поддерживаемых ими систем. Объекты поддерживающих услуг необходимо регулярно проверять и тестировать для обеспечения уверенности в их должном функционировании и уменьшения любого риска, связанного с их неисправной работой или отказом. Необходимо обеспечить надлежащую подачу электропитания, соответствующую спецификациям производителя оборудования.

Оборудование, поддерживающее важнейшие процессы бизнеса, рекомендуется подключать через источники бесперебойного электропитания (ИБП), чтобы обеспечить его безопасное выключение и (или) непрерывное функционирование. В планах обеспечения непрерывности электроснабжения следует предусмотреть действия на случай отказа ИБП. Резервный генератор следует использовать, когда функционирование оборудования необходимо обеспечить во время длительного отказа подачи электроэнергии. Для обеспечения работы генератора в течение длительного времени необходимо обеспечить соответствующую поставку топлива. Оборудование ИБП и генераторы должны регулярно проверяться, чтобы обеспечить уверенность в наличии адекватной производительности, а также тестироваться в соответствии с рекомендациями производителя. Кроме того, следует обращать внимание на использование нескольких источников питания или, если организация большая, отдельной электроподстанции.

Аварийные выключатели электропитания необходимо расположить около запасных выходов помещений, в которых находится оборудование, чтобы ускорить отключение электропитания в критических ситуациях. Необходимо обеспечить работу аварийного освещения на случай отказа электропитания, потребляемого от сети.

Водоснабжение должно быть стабильным и адекватным для обеспечения кондиционирования воздуха, обеспечения работы устройств увлажнения и систем пожаротушения (там, где они используются). Неисправности в работе системы водоснабжения могут привести к повреждению оборудования или могут препятствовать эффективной работе системы пожаротушения. Следует оценивать необходимость установки системы сигнализации для обнаружения неправильного функционирования объектов поддерживающих услуг.

Связь телекоммуникационного оборудования с оборудованием провайдера услуг должна осуществляться, по меньшей мере, по двум различным маршрутам, чтобы предотвратить отказ в одном из соединительных маршрутов, который может сделать услугу по передаче речи невозможной. Услуги по передаче речи должны быть адекватными, чтобы удовлетворять местным законодательным требованиям в отношении аварийной связи.

Вариантом достижения непрерывности электропитания будет наличие нескольких источников питания, что позволит избежать единой точки отказа в электропитании.

Безопасность кабельной сети

Силовые и телекоммуникационные кабельные сети, по которым передаются данные или поддерживающие информационные услуги, необходимо защищать от перехвата информации или разрушения.

В отношении безопасности кабельной сети следует рассмотреть следующие рекомендации:

a) силовые и телекоммуникационные линии, связанные со средством обработки информации, должны, по возможности, располагаться под землей или иметь адекватную альтернативную защиту;

b) сетевой кабель должен быть защищен от неавторизованных подключений или повреждения, например посредством использования специального кожуха или выбора маршрутов прокладки кабеля в обход общедоступных участков;

c) силовые кабели должны быть отделены от коммуникационных, чтобы предотвращать помехи;

d) следует использовать кабель и оборудование с четкой маркировкой, чтобы свести к минимуму эксплуатационные ошибки, например случайного внесения исправлений при ремонте сетевых кабелей;

e) для уменьшения вероятности ошибок следует использовать документально оформленный перечень исправлений;

f) дополнительные меры и средства контроля и управления для чувствительных или критических систем включают:

1) использование армированного кабельного канала, а также закрытых помещений или шкафов в контрольных и конечных точках;

2) использование дублирующих маршрутов прокладки кабеля и (или) альтернативных способов передачи, обеспечивающих соответствующую безопасность;

3) использование оптико-волоконных линий связи;

4) использование электромагнитного экранирования для защиты кабелей;

5) проведение технических осмотров и физических проверок подключения неавторизованных устройств к кабельной сети;

6) управляемый доступ к коммутационным панелям и электрощитовым.

Техническое обслуживание оборудования

Должно проводиться надлежащее техническое обслуживание оборудования для обеспечения его непрерывной доступности и целостности.

В отношении технического обслуживания оборудования следует рассмотреть следующие рекомендации:

a) оборудование должно обслуживаться в соответствии с рекомендуемыми поставщиком периодичностью и спецификациями;

b) техническое обслуживание и ремонт оборудования должны проводиться только авторизованным персоналом;

c) следует хранить записи обо всех предполагаемых или фактических неисправностях и всех видах профилактического обслуживания;

d) если запланировано техническое обслуживание оборудования, следует принимать соответствующие меры и средства контроля и управления, при этом необходимо учитывать, будет ли техническое обслуживание проводиться персоналом организации или за ее пределами; при необходимости, чувствительная информация из оборудования должна быть удалена, или специалисты по техническому обслуживанию и ремонту должны иметь соответствующий допуск;

e) должны соблюдаться все требования, устанавливаемые полисами страхования.

Безопасность оборудования вне помещений организации

При обеспечении безопасности оборудования, используемого вне места его постоянной эксплуатации, следует учитывать различные риски, связанные с работой вне помещений организации.

Независимо от права собственности использование оборудования для обработки информации вне помещений организации должно быть санкционировано руководством.

Следующие рекомендации необходимо учитывать в отношении защиты оборудования, используемого вне помещений организации:

a) оборудование и носители информации, взятые из помещений организации, не следует оставлять без присмотра в общедоступных местах; во время поездок портативные компьютеры нужно перевозить как ручную кладь и по возможности маскировать;

b) необходимо соблюдать инструкции изготовителей по защите оборудования, например по защите от воздействия сильных электромагнитных полей;

c) для работы на дому следует определить соответствующие меры и средства контроля и управления, исходя из оценки рисков, например использование запираемых шкафов для хранения документов, соблюдение политики "чистого стола", управление доступом к компьютерам и связь с офисом по защищенным сетям (см. также ИСО/МЭК 18028 "Сетевая Безопасность");

d) с целью защиты оборудования, используемого вне помещений организации, должно проводиться адекватное страхование, покрывающее указанные риски.

Риски безопасности, например связанные с повреждением, воровством и подслушиванием, могут значительно отличаться для различных объектов и должны учитываться при определении наиболее подходящих мер и средств контроля и управления.

Под оборудованием, используемым для обработки и хранения информации, понимаются все типы персональных компьютеров, электронных записных книжек, мобильных телефонов, смарт-карт, а также бумага или другие виды носителей информации, которые применяются для работы на дому или транспортируются за пределы обычных рабочих помещений.

Безопасная утилизация или повторное использование оборудования

Все компоненты оборудования, содержащие носители данных, следует проверять с целью обеспечения уверенности в том, что любые чувствительные данные и лицензионное программное обеспечение были удалены или перезаписаны безопасным образом до их утилизации.

Носители данных, содержащие чувствительную информацию, необходимо физически уничтожать, или информацию необходимо разрушить, удалить или перезаписать способами, делающими исходную информации невосстановимой, а не использовать стандартные функции удаления и форматирования.

Поврежденные устройства, содержащие чувствительные данные, могут потребовать проведения оценки рисков с целью определения элементов, которые должны быть физически разрушены, направлены на ремонт или игнорированы.

Информация может быть скомпрометирована вследствие небрежной утилизации или повторного использования оборудования

Перемещение имущества

Оборудование, информацию или программное обеспечение можно использовать вне помещений организации только при наличии соответствующего разрешения.

Необходимо учитывать следующие рекомендации:

a) оборудование, информацию или программное обеспечение можно использовать вне помещений организации только при наличии соответствующего разрешения;

b) сотрудники, подрядчики и представители третьей стороны, имеющие право разрешать перемещение активов за пределы места эксплуатации, должны быть четко определены;

c) сроки перемещения оборудования должны быть установлены и проверены на соответствие при возврате;

d) там, где необходимо и уместно, оборудование следует регистрировать при перемещении из помещений организации и при возврате

Выборочные проверки, проводимые для обнаружения неавторизованного перемещения имущества, также могут проводиться для обнаружения неавторизованных устройств регистрации, оружия и т.д., и предотвращения их вноса в помещения организации. Такие выборочные проверки необходимо выполнять согласно соответствующим законам и инструкциям. Сотрудники должны быть осведомлены о проведении выборочных проверок, а проверки должны проводиться только с разрешения соответствующего правовым и нормативным требованиям.