ЛЕКЦИЯ 4: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ПРИ РАБОТЕ СО СТОРОННИМИ ОРГАНИЗАЦИЯМИ И ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АКТИВОВ ОРГАНИЗАЦИИ

1 вопрос: Идентификация рисков, являющихся следствием работы со сторонними организациями

Цель: Обеспечивать безопасность информации и средств обработки информации организации при доступе, обработке, передаче и менеджменте, осуществляемом сторонними организациями.
Безопасность информации и средств обработки информации организации не должна снижаться при вводе продуктов или сервисов сторонних организаций.
Доступ сторонних организаций к средствам обработки информации организации, а также к обработке и передаче информации должен находиться под контролем.
Если имеется потребность бизнеса в работе со сторонними организациями, которым может потребоваться доступ к информации и средствам обработки информации организации, а также в получении или обеспечении продукта или сервиса от сторонней организации или для нее, следует выполнять оценку риска для определения последствий для безопасности и требований к мерам и средствам контроля и управления. Меры и средства контроля и управления следует согласовывать и определять в контракте со сторонней организацией

Мера и средство контроля и управления: риски для информации и средств обработки информации организации, являющиеся следствием процессов бизнеса, в которых участвуют сторонние организации, необходимо определять и необходимо реализовывать соответствующие меры и средства контроля и управления прежде, чем будет предоставлен доступ.

Там, где есть необходимость разрешения доступа сторонней организации к средствам обработки информации или информации организации, следует проводить оценку риска с целью определения каких-либо потребностей в специальных мерах и средствах контроля и управления. При определении рисков, связанных с доступом сторонних организаций, следует учитывать:

a) средства обработки информации, необходимые сторонним организациям для доступа;

b) тип доступа к информации и средствам обработки информации, который будет предоставлен сторонним организациям, например:

1) физический доступ, например к офисам, машинным залам, картотекам;

2) логический доступ, например к базам данных, информационным системам организации;

3) возможность сетевого соединения между сетью (сетями) организации и сторонней организации, например неразъемное соединение, удаленный доступ;

4) осуществление доступа на месте или вне места эксплуатации;

c) ценность и чувствительность используемой информации, ее критичность для операций бизнеса;

d) меры и средства контроля и управления, необходимые для защиты информации, не предназначенной для доступа сторонним организациям;

e) персонал сторонней организации, участвующий в обработке информации организации;

f) каким образом организация или персонал, авторизованные на получение доступа, могут быть идентифицированы, авторизация проверена и как часто это необходимо подтверждать;

g) различные способы и меры и средства контроля и управления, применяемые сторонними организациями при хранении, обработке, передаче, совместном использовании и обмене информацией;

h) влияние непредоставления требуемого доступа сторонней организации и ввода или получения сторонней организацией неточной или ложной информации;

i) инструкции и процедуры принятия мер в отношении инцидентов информационной безопасности и возможных убытков, а также сроки и условия возобновления доступа сторонних организаций в случае инцидента информационной безопасности;

j) правовые и нормативные требования, а также договорные обязательства, значимые для сторонних организаций, которые необходимо принимать в расчет;

k) влияние вышеназванных мер на интересы каких-либо других причастных сторон.

Доступ сторонних организаций к информации организации не должен обеспечиваться до тех пор, пока не будут реализованы соответствующие меры и средства контроля и управления и пока не будет подписан договор, определяющий сроки и условия подключения или доступа и рабочий механизм. Как правило, все требования к безопасности, вытекающие из работы со сторонними организациями или внутреннего контроля, должны отражаться в соглашении со сторонними организациями

Следует обеспечивать уверенность в том, что сторонние организации осведомлены о своих обязанностях, и берут на себя ответственность и обязательства в отношении доступа, обработки, передачи или менеджмента информации и средств обработки информации организации

Информация может быть подвергнута риску сторонними организациями, в которых менеджмент безопасности осуществляется неадекватным образом. Должны определяться и применяться меры и средства контроля и управления с целью администрирования доступа сторонней организации к средствам обработки информации. Например там, где имеется определенная потребность в конфиденциальности информации, могут быть использованы соглашения о неразглашении.

Организации могут сталкиваться с рисками, связанными с межорганизационными процессами, менеджментом и связью в том случае, если применяется большой процент аутсорсинга , или если к участию привлекаются несколько сторонних организаций.

Меры и средства контроля и управления охватывают различные мероприятия с привлечением сторонних организаций, включающие:

a) провайдеров услуг, например Интернет-провайдеров, сетевых провайдеров, услуги телефонной связи, технического обслуживания и поддержки;

b) услуги по менеджменту безопасности;

c) клиентов;

d) аутсорсинг средств и (или) операций, например систем ИТ, услуг по сбору данных, операций центра телефонного обслуживания;

e) консультантов по вопросам менеджмента и бизнеса, а также аудиторов;

f) разработчиков и поставщиков, например программных продуктов и систем ИТ;

g) уборку, общественное питание и другие вспомогательные услуги, обеспечиваемые в рамках договоров аутсорсинга;

h) временных работников, прием на работу студентов и другие нерегулярные краткосрочные назначения.

Такие соглашения могут помочь снизить риски, связанные с привлечением сторонних организаций.

Рассмотрение вопросов безопасности при работе с клиентами:

Все установленные требования безопасности должны быть рассмотрены прежде, чем клиентам будет дан доступ к информации или активам организации.

Следующие условия должны быть учтены при рассмотрении безопасности до предоставления клиентам доступа к какому-либо активу организации (в зависимости от типа и продолжительности предоставляемого доступа не все из них могут быть применимы):

а) защита активов, включая:

1) процедуры защиты активов организации, в том числе информацию и программное обеспечение, а также менеджмент известных уязвимостей;

2) процедуры для определения компрометации активов, например вследствие потери или модификации данных;

3) целостность;

4) ограничения на копирование и разглашение информации;

b) описание продукта или услуги, которые должны быть обеспечены;

c) различные причины, требования и преимущества, связанные с доступом клиента;

d) политика управления доступом, охватывающая:

1) разрешенные методы доступа, а также управление и использование уникальных идентификаторов, типа идентификаторов пользователя и паролей;

2) процесс авторизации в отношении доступа и привилегий пользователей;

3) положение о том, что весь доступ, не авторизованный явным образом, является запрещенным;

4) процесс отмены прав доступа или прерывание соединения между системами;

e) процедуры в отношении отчетности, уведомления и расследования неточностей в информации (например персональных подробностей), инцидентов информационной безопасности и нарушений безопасности;

f) описание каждой предоставляемой услуги;

g) определение необходимого и неприемлемого уровня обслуживания;

h) право на проведение мониторинга и отмену какой-либо деятельности, связанной с активами организации;

i) соответствующие обязательства организации и клиента;

j) обязательства относительно юридических вопросов, и способ обеспечения уверенности в соответствии правовым нормам, например законодательству о защите данных, особенно с учетом различных требований национальных правовых систем, если договор предполагает сотрудничество с клиентами в других странах ;

к) соблюдение прав на интеллектуальную собственность и авторских прав, а также обеспечение правовой защиты любой совместной работы и

Требования безопасности в отношении клиентов, осуществляющих доступ к активам организации, могут варьироваться в значительной степени в зависимости от средств обработки информации и информации, к которой осуществляется доступ. Такие требования безопасности могут быть рассмотрены с использованием договоров с клиентами, в которых содержатся все установленные риски и требования безопасности .

По договорам со сторонними организациями могут также привлекаться другие участники. В договорах, предоставляющих доступ сторонней организации, должно содержаться разрешение на привлечение других организаций, а также условия их доступа и участия.

Рассмотрение требований безопасности в договорах с третьей стороной

Договоры с третьей стороной, привлеченной к доступу, обработке, передаче или управлению информацией или средствами обработки информации организации, или к дополнению продуктов или услуг к средствам обработки информации, должны охватывать все соответствующие требования безопасности. Договор должен обеспечивать уверенность в том, что нет никакого недопонимания между организацией и третьей стороной. Организации должны убедиться, что третья сторона сможет возместить возможные убытки.

Следующие условия должны быть рассмотрены на предмет включения в договор с целью удовлетворения установленных требований безопасности :

a) политика информационной безопасности;

b) меры и средства контроля и управления для обеспечения уверенности в защите активов, включая:

1) процедуры по защите активов организации, в том числе информацию, программное обеспечение и аппаратные средства;

2) какие-либо меры и средства контроля и управления, а также инструменты необходимой физической защиты;

3) меры и средства контроля и управления для обеспечения уверенности в защите от вредоносного программного средства;

4) процедуры по определению компрометации активов, например вследствие потери или модификации информации, программного обеспечения и аппаратных средств;

5) меры и средства контроля и управления по обеспечению уверенности в возврате или уничтожении информации и активов по окончании договора или в согласованное время в течение срока действия договора;

6) конфиденциальность, целостность, доступность и любое другое значимое свойство активов;

7) ограничения на копирование и разглашение информации, и применение соглашений о конфиденциальности ;

c) тренинг пользователей и администраторов в отношении методов, процедур и безопасности;

d) обеспечение осведомленности пользователей в отношении обязанностей и вопросов, связанных с информационной безопасностью;

e) обеспечение доставки персонала к месту работы, где это необходимо;

f) обязанности, касающиеся установки и сопровождения аппаратных средств и программного обеспечения;

g) четкая структура подотчетности и согласованные форматы представления отчетов;

h) ясный и определенный процесс менеджмента изменений;

i) политика управления доступом, охватывающая:

1) различные причины, требования и преимущества, делающие доступ третьей стороны необходимым;

2) разрешенные методы доступа, а также управление и использование уникальных идентификаторов типа идентификаторов пользователя и паролей;

3) процесс авторизации в отношении доступа и привилегий пользователей;

4) требование по ведению списка лиц, уполномоченных использовать предоставляемые услуги, с указанием соответствующих прав и привилегий;

5) положение о том, что весь доступ, не авторизованный явным образом, является запрещенным;

6) процесс отмены прав доступа или прерывание соединения между системами;

j) процедуры в отношении отчетности, уведомления и расследования инцидентов информационной безопасности и нарушений безопасности, а также нарушений требований, изложенных в соглашении;

к) описание продукта или услуги, которые должны быть предоставлены, и описание информации, которая должна быть предоставлена, наряду с категорией ее секретности ;

l) определение необходимого и неприемлемого уровня обслуживания;

m) определение поддающихся контролю критериев эффективности, а также их мониторинг и предоставление отчетности;

n) право на проведение мониторинга и отмену любой деятельности в отношении активов организации;

o) право на проведение аудита исполнения договорных обязательств и возможность проведения такого аудита третьей стороной, а также перечисление установленных законом прав аудиторов;

p) установление процесса информирования о возникающих проблемах с целью их разрешения;

q) требования в отношении непрерывности обслуживания, включая меры по обеспечению доступности и надежности, в соответствии с приоритетами бизнеса организации;

r) соответствующие обязательства сторон в рамках соглашения;

s) обязательства относительно юридических вопросов, и способов обеспечения уверенности в соответствии правовым требованиям, например законодательству о защите данных, особенно с учетом различных требований национальных правовых систем, если договор предполагает сотрудничество с клиентами в других странах

t) соблюдение прав на интеллектуальную собственность и авторских прав , а также обеспечение правовой защиты любой совместной работы ;

u) привлечение третьей стороны вместе с субподрядчиками, меры и средства контроля и управления безопасности, которые эти субподрядчики должны реализовать;

v) условия перезаключения/окончания договоров:

1) план действий в чрезвычайных ситуациях должен содержать положения на случай, если какая-либо сторона пожелает прервать отношения до окончания срока действия договоров;

2) перезаключение договоров в случае изменения требований организации к безопасности;

3) действующие документированные перечни активов, лицензий, договоров или связанных с ними прав.

Договоры могут варьироваться в значительной мере в отношении различных организаций и среди различных типов третьих сторон. Поэтому следует заботиться о включении в договоры всех определенных рисков и требований безопасности . При необходимости требуемые меры и средства контроля и управления, а также процедуры могут быть расширены в плане менеджмента безопасности.

Если менеджмент информационной безопасности осуществляется в рамках договоров аутсорсинга, то в договорах должно быть оговорено, каким образом третья сторона будет гарантировать поддержание адекватной безопасности, определенной оценкой риска, а также адаптацию к выявленным рискам и изменениям рисков.

Некоторые из различий между аутсорсингом и другими формами обеспечения услуг третьими сторонами включают в себя вопросы ответственности, планирование переходного периода и возможного срыва операций в течение данного периода, планирование мероприятий на случай непредвиденных ситуаций и тщательность проверок, а также сбор и управление информацией по инцидентам безопасности. Поэтому важно, чтобы организация планировала и управляла переходом к договорам аутсорсинга, и применяла соответствующий процесс менеджмента изменений и перезаключения/окончания действия договоров.

В договоре необходимо учитывать процедуры непрерывной обработки на случай, если третья сторона окажется неспособной поставлять свои услуги, для предотвращения какой-либо задержки по организации замены услуг.

В договорах с третьими сторонами могут участвовать также и другие стороны. Договоры, предоставляющие доступ третьим сторонам, должны содержать разрешение на привлечение других организаций, а также условия их доступа и участия.

Как правило, договоры разрабатываются, в первую очередь, организацией. Иногда договор может быть разработан и предложен организации третьей стороной. Организации необходимо обеспечивать уверенность в том, что требования третьей стороны, изложенные в предлагаемых договорах, не оказывают излишнего влияния на ее собственную безопасность.

2 вопрос Информационная безопасность активов предприятия

Цель: Обеспечить соответствующую защиту активов организации.

Все активы должны учитываться и иметь назначенного владельца.

Необходимо определять владельцев всех активов, и следует определять ответственного за поддержку соответствующих мер и средств контроля и управления. Реализация определенных мер и средств контроля и управления при необходимости может быть делегирована владельцем, но владелец остается ответственным за надлежащую защиту активов.

Все активы должны быть четко определены, должна составляться и поддерживаться опись всех важных активов. Организации следует идентифицировать все активы и документально оформлять значимость этих активов. В опись активов следует включить всю информацию, необходимую для восстановления после бедствия, в том числе тип актива, формат, местоположение, информацию о резервных копиях, информацию о лицензировании и ценности для бизнеса. Опись не должна без необходимости дублировать другие описи, но следует обеспечивать уверенность в том, что ее содержание выверено.

Кроме того, владение и классификация информации должны быть согласованы и документально оформлены в отношении каждого актива. Основываясь на важности актива, его ценности для бизнеса и его категории секретности, надлежит определить уровни защиты, соответствующие значимости активов (более подробную информацию о том, как оценивать активы, чтобы учесть их важность, можно найти в ИСО/МЭК 27005).

Существует много типов активов, включающих:

a) информацию: базы данных и файлы данных, договоры и соглашения, системная документация, исследовательская информация, руководства пользователя, учебные материалы, процедуры эксплуатации или поддержки, планы непрерывности бизнеса, меры по переходу на аварийный режим, контрольные записи и архивированная информация;

b) программные активы: прикладные программные средства, системные программные средства, средства разработки и утилиты;

c) физические активы: компьютерное оборудование, средства связи, съемные носители информации и другое оборудование;

d) услуги: вычислительные услуги и услуги связи, основные поддерживающие услуги, например отопление, освещение, электроэнергия и кондиционирование воздуха;

e) персонал, его квалификация, навыки и опыт;

f) нематериальные ценности, например репутация и имидж организации.

Описи активов помогают обеспечивать уверенность в том, что активы организации эффективно защищены, данные описи могут также потребоваться для других целей, таких как обеспечение безопасности труда, страховые или финансовые (менеджмент активов) вопросы. Процесс инвентаризации активов - важное условие для менеджмента риска

Владение активами

Вся информация и активы, связанные со средствами обработки информации должны находиться во владении определенной части организации.

Владелец актива должен нести ответственность за:

a) обеспечение уверенности в том, что информация и активы, связанные со средствами обработки информации, классифицированы соответствующим образом;

b) определение и периодический пересмотр ограничений и классификаций доступа, принимая в расчет применимые политики управления доступом. Владение может распространяться на:

a)процесс бизнеса;

b) определенный набор деятельностей;

c) прикладные программы;

d) определенное множество данных.

Повседневные задачи могут быть переданы, например должностному лицу, ежедневно работающему с активом, но ответственность сохраняется за владельцем.

В сложных информационных системах рекомендуется обозначить группы активов, действующих вместе, для обеспечения определенной функции, такой как "услуга". В данном случае владелец услуг является ответственным за поставку услуги и функционирование активов, которые обеспечивают данную услугу.

Приемлемое использование активов

Мера и средство контроля и управления

Следует определять, документально оформлять и реализовывать правила приемлемого использования информации и активов, связанных со средствами обработки информации.

Всем служащим, подрядчикам и представителям третьей стороны рекомендуется следовать правилам приемлемого использования информации и активов, связанных со средствами обработки информации, включая:

a) правила использования электронной почты и Интернета;

b) рекомендации по использованию мобильных устройств, особенно в отношении использования их за пределами помещений организации.

Соответствующему управленческому персоналу должны быть предоставлены конкретные правила или рекомендации. Служащие, подрядчики и представители третьей стороны, использующие или имеющие доступ к активам организации, должны быть осведомлены о существующих ограничениях в отношении использования ими информации и активов организации, связанных со средствами обработки информации и ресурсами. Они должны нести ответственность за использование ими любых средств обработки информации, и любое использование таких средств осуществлять под свою ответственность.

Классификация информации

Цель: Обеспечить уверенность в защищенности информации на надлежащем уровне.

Информацию следует классифицировать, чтобы определить необходимость, приоритеты и предполагаемую степень защиты при обработке информации. Информация имеет различные степени чувствительности и критичности. Некоторые элементы могут потребовать дополнительного уровня защиты или специальной обработки. Схему классификации информации следует использовать для определения соответствующего множества уровней защиты и установления потребности в принятии специальных мер обработки.

Рекомендации по классификации

Информацию следует классифицировать, исходя из ее ценности, законодательных требований, чувствительности и критичности для организации.

При классификации информации и связанных с ней защитных мер и средств контроля и управления необходимо учитывать требования бизнеса в отношении совместного использования или ограничения доступа к информации и последствия для бизнеса, связанные с такими требованиями

Рекомендации по классификации должны включать руководящие указания по начальной классификации и последующей классификации по истечении времени в соответствии с некой предопределенной политикой управления доступом.

В обязанности владельца актива входит классификация актива, ее периодический пересмотр и обеспечение уверенности в том, что она поддерживается на актуальном и соответствующем уровне

Предметом рассмотрения должно стать количество классификационных категорий и преимущества, получаемые от их использования. Чрезмерно сложные схемы могут стать обременительными и неоправданно дорогими для применения, или могут оказаться неосуществимыми. Следует проявлять осторожность в интерпретации классификационных меток на документах из других организаций, так как одни и те же метки могут иметь различный смысл.

Уровень защиты может оцениваться с помощью анализа конфиденциальности, целостности и доступности, а также каких-либо других требований в отношении рассматриваемой информации.

Информация часто перестает быть чувствительной или критической по истечении некоторого периода времени, например когда она делается общедоступной. Эти аспекты необходимо принимать во внимание, поскольку присвоение более высокой категории может привести к реализации ненужных мер и средств контроля и управления и, как следствие, к дополнительным расходам.

При назначении классификационных уровней, совместное рассмотрение документов с аналогичными требованиями безопасности может упростить задачу по классификации.

Маркировка и обработка информации

Соответствующий набор процедур маркировки и обработки информации следует разрабатывать и реализовывать в соответствии с системой классификации, принятой организацией.

Необходимо, чтобы процедуры маркировки информации охватывали информационные активы, представленные как в физической, так и в электронной форме.

Выводимые из систем документы, содержащие информацию, которая классифицирована как чувствительная или критическая, должны содержать соответствующий маркировочный знак. Маркированными могут быть напечатанные отчеты, экранные отображения, носители информации (например ленты, диски, компакт-диски), электронные сообщения и пересылаемые файлы.

Для каждого уровня классификации должны быть определены процедуры обработки, включающие безопасную обработку, хранение, передачу, снятие грифа секретности и уничтожение. Сюда следует также отнести процедуры по обеспечению сохранности и регистрации любого события, имеющего значение для безопасности.

Договоры с другими организациями, включающие требования о совместном использовании информации, должны содержать процедуры определения классификации этой информации и интерпретации классификационных меток других организаций.

Маркировка и безопасная обработка классифицированной информации является ключевым требованием для соглашений о совместном использовании информации. Физические метки являются наиболее распространенной формой маркировки. Однако некоторые информационные активы, например документы в электронной форме, не могут быть маркированы физически, и поэтому необходимо использовать электронные аналоги маркировки. Например на экране или дисплее может появиться уведомляющая метка. Там, где маркировка неосуществима, применяют другие средства обозначения классификации информации, например с помощью процедур или метаданных.