Методы и средства обеспечения безопасности.

1. Понятие информационной безопасности

Информация - это актив, который, подобно другим активам организации, имеет ценность и, следовательно, должен быть защищен надлежащим образом, что важно для среды бизнеса, где наблюдается все возрастающая взаимосвязь. Как результат такой все возрастающей взаимосвязи, информация в настоящее время подвергается растущему числу и более широкому спектру угроз и уязвимостей по обеспечению безопасности информационных систем и сетей.

Информация может существовать в различных формах: быть напечатанной или написанной на бумаге, храниться в электронном виде, передаваться по почте или с использованием электронных средств связи, демонстрироваться на пленке или выражена устно. Независимо от формы представления информации, средств ее распространения или хранения, она всегда должна быть адекватно защищена.

Информационная безопасность защищает информацию от широкого диапазона угроз с целью обеспечения уверенности в непрерывности бизнеса, минимизации риска бизнеса, получения максимальной отдачи от инвестиций, а также реализации потенциальных возможностей бизнеса.

Информационная безопасность достигается путем реализации соответствующего комплекса мер и средств контроля и управления, которые могут быть представлены политиками, процессами, процедурами, организационными структурами, а также функциями программных и аппаратных средств. Указанные меры и средства контроля и управления необходимо создавать, реализовывать, подвергать мониторингу, анализировать и улучшать, если необходимо, для обеспечения уверенности в том, что определенная безопасность и определенные цели бизнеса организации достигнуты. Все это необходимо выполнять наряду с другими процессами менеджмента бизнеса.

Информация и поддерживающие ее процессы, системы и сети являются важными деловыми активами. Определение, достижение, поддержка и улучшение информационной безопасности могут быть существенными аспектами для поддержания конкурентоспособности, денежного оборота, доходности, соблюдения законов и коммерческого имиджа.

Организация должна определить свои требования к информационной безопасности. Существуют три основных источника требований безопасности.

Первый источник складывается из оценки рисков организации, принимая во внимание общую стратегию и цели бизнеса организации. Посредством оценки рисков идентифицируются угрозы активам организации, оцениваются уязвимости и вероятности возникновения угроз, а также оцениваются возможные последствия.

Вторым источником являются правовые, законодательные, нормативные и договорные требования, которым должны удовлетворять организация, ее торговые партнеры, подрядчики и поставщики услуг, а также их социокультурная среда.

Третьим источником является определенный набор принципов, целей и требований бизнеса для обработки информации, которые разработала организация для поддержки своей деятельности.

Оценка рисков безопасности

Требования безопасности определяются с помощью систематической оценки рисков. Расходы на меры и средства контроля и управления должны быть соизмеримы с возможным ущербом бизнесу в результате отказа от обеспечения безопасности.

Результаты оценки рисков помогут в определении конкретных мер и приоритетов в области менеджмента рисков информационной безопасности, а также внедрению мер и средств контроля и управления, выбранных для защиты от этих рисков.

Оценка рисков должна периодически повторяться, чтобы учитывать любые изменения, которые могли бы повлиять на результаты оценки риска.

Выбор мер и средств контроля и управления

После того как были определены требования к безопасности и риски безопасности и приняты решения в отношении обработки рисков, следует выбрать и внедрить такие меры и средства контроля и управления, которые обеспечат уверенность в снижении рисков до приемлемого уровня. Меры и средства контроля и управления могут быть выбраны из настоящего документа и других источников, а также могут быть разработаны новые меры и средства контроля и управления, удовлетворяющие специфическим потребностям организации. Выбор мер и средств контроля и управления зависит от решений организации, основанных на критериях принятия рисков, вариантах обработки рисков и общем подходе к менеджменту рисков, применяемом в организации. При этом необходимо также учитывать все соответствующие национальные и международные законы и нормы.

Отправная точка информационной безопасности

Отдельные меры и средства контроля и управления могут рассматриваться как подходящая отправная точка информационной безопасности. Такие меры и средства контроля и управления либо основываются на ключевых требованиях законодательства, либо рассматриваются как общепринятая практика в области информационной безопасности.

Ключевыми мерами и средствами контроля и управления, с точки зрения законодательства, для организации являются:

a) защита данных и конфиденциальность персональных данных

b) защита документов организации

c) обязанностей по обеспечению информационной безопасности;

c) осведомленность права на интеллектуальную собственность

Меры и средства контроля и управления, рассматриваемые как общепринятая практика в области информационной безопасности, включают:

a) документирование политики информационной безопасности;

b) распределение, обучение и тренинг в области информационной безопасности;

d) корректирующая обработка в прикладных программах;

e) менеджмент технических уязвимостей;

f) менеджмент непрерывности бизнеса;

g) менеджмент инцидентов информационной безопасности и необходимое совершенствование

Перечисленные меры и средства контроля и управления применимы для большинства организаций и сред.

Следует отметить, что хотя все меры и средства контроля и управления, приведенные в настоящем документе, являются важными, уместность какой-либо меры и средства контроля и управления должна определяться в свете конкретных рисков, с которыми сталкивается организация. Следовательно, несмотря на то, что вышеописанный подход рассматривается как отправная точка информационной безопасности, он не заменяет выбор мер и средств контроля и управления, основанный на оценке рисков.

Важнейшие факторы успеха

Практика показывает, что для успешного внедрения информационной безопасности в организации решающими факторами зачастую являются следующие:

a) соответствие целей, политик и процедур информационной безопасности целям бизнеса;

b) подход и основы для внедрения, поддержки, мониторинга и улучшения информационной безопасности, которые согласуются с корпоративной культурой;

c) видимая поддержка и обязательства со стороны руководства всех уровней;

d) четкое понимание требований информационной безопасности, оценки рисков и менеджмента рисков;

e) эффективный маркетинг информационной безопасности среди всех руководителей, сотрудников и других сторон для достижения осведомленности;

f) распространение руководящих указаний политики информационной безопасности и соответствующих стандартов среди всех руководителей, сотрудников и других сторон;

g) обеспечение финансирования деятельностей по менеджменту информационной безопасности;

h) обеспечение соответствующей осведомленности, обучения и тренинга;

i) создание эффективного процесса менеджмента инцидентов информационной безопасности;

j) внедрение системы измерений***, используемых для оценивания эффективности менеджмента информационной безопасности и предложений по улучшению.

2. Оценка и обработка рисков

1. Оценка рисков безопасности

Оценка рисков должна идентифицировать риски, определить количество и приоритеты рисков на основе критериев для принятия риска и целей, значимых для организации. Результаты должны служить ориентиром и определять соответствующие действия руководства и приоритеты менеджмента рисков информационной безопасности, а также реализацию мер и средств контроля и управления, выбранных для защиты от этих рисков. Может возникнуть необходимость в неоднократном выполнении процесса оценки рисков и выбора мер и средств контроля и управления для того, чтобы охватить различные подразделения организации или отдельные информационные системы.

Оценка рисков должна включать систематический подход, заключающийся в количественной оценке рисков (анализ риска), и процесс сравнения количественно оцененных рисков с данными критериями рисков для определения значимости рисков (оценивание рисков).

Оценки рисков следует выполнять периодически, чтобы учитывать изменения в требованиях безопасности и в ситуации, связанной с риском, например в отношении активов, угроз, уязвимостей, воздействий, оценивания рисков, а также при значительных изменениях. Такие оценки рисков следует проводить систематически, способом, дающим сравнимые и воспроизводимые результаты.

2. Обработка рисков безопасности

Прежде чем рассмотреть обработку некоего риска, организация должна выбрать критерии определения приемлемости или неприемлемости рисков. Риски могут быть приняты, если, например они оцениваются как низкие, или когда стоимость обработки невыгодна для организации. Такие решения необходимо регистрировать.

В отношении каждого из выявленных рисков, вслед за оценкой рисков, необходимо принимать решение по его обработке. Возможные варианты обработки рисков включают в себя:

a) применение соответствующих мер и средств контроля и управления для снижения рисков;

b) сознательное и объективное принятие рисков в том случае, если они, несомненно, удовлетворяют политике и критериям организации в отношении принятия рисков;

c) предотвращение рисков путем недопущения действий, которые могут стать причиной возникновения рисков;

d) перенос взаимодействующих рисков путем разделения их с другими сторонами, например страховщиками или поставщиками.

Меры и средства контроля и управления могут быть выбраны из настоящего стандарта или других совокупностей мер и средств контроля и управления, могут быть созданы новые меры и средства контроля и управления с целью удовлетворения специфических потребностей организации. Необходимо признать, что некоторые меры и средства контроля и управления не могут быть применены для каждой информационной системы или среды, и не могут быть применены для всех организаций. В качестве примера в описывается, как обязанности могут быть разделены, чтобы предотвратить мошенничество и ошибки. В небольших организациях может отсутствовать возможность разделения всех обязанностей, и могут потребоваться другие способы достижения той же самой цели управления.

Меры и средства контроля и управления информационной безопасности должны рассматриваться на этапе спецификации и разработки системных и проектных требований. Отказ от этого может приводить к дополнительным расходам и менее эффективным решениям, а в худшем случае, к неспособности достижения адекватной безопасности.

Следует иметь в виду, что никакая совокупность мер и средств контроля и управления не может достигать полной безопасности, и что необходимо реализовывать дополнительные действия по менеджменту, чтобы осуществлять мониторинг, оценку и повышение действенности и эффективности мер и средств контроля и управления безопасности для поддержки целей организации.

3. Политика безопасности

1. Политика информационной безопасности

Целью политики информационной безопасности является обеспечение управления и поддержка высшим руководством информационной безопасности в соответствии с требованиями бизнеса и соответствующими законами и нормами

Высшее руководство должно установить четкое направление политики в соответствии с целями бизнеса и демонстрировать поддержку и обязательства в отношении обеспечения информационной безопасности посредством разработки и поддержки политики информационной безопасности в рамках организации.

При необходимости следует предусмотреть наличие контактного лица, занимающегося вопросами информационной безопасности внутри организации, к которому могут обращаться заинтересованные сотрудники. Следует налаживать контакты с внешними специалистами по безопасности или группами специалистов, включая соответствующие органы, чтобы находиться в курсе отраслевых тенденций, осуществлять мониторинг стандартов и методов оценки, и обеспечивать адекватные точки контакта при обработке инцидентов информационной безопасности. Следует поощрять многопрофильный подход к обеспечению информационной безопасности.

2.Документирование политики информационной безопасности

Политика информационной безопасности должна устанавливать ответственность руководства, а также излагать подход организации к менеджменту информационной безопасности, Документ, в котором излагается политика, должен содержать положения относительно:

a) определения информационной безопасности, ее общих целей и сферы действия, а также упоминания значения безопасности как инструмента, обеспечивающего возможность совместного использования информации;

b) изложения намерений руководства, поддерживающих цели и принципы информационной безопасности в соответствии со стратегией и целями бизнеса;

c) подхода к установлению мер и средств контроля и управления и целей их применения, включая структуру оценки риска и менеджмента риска;

d) краткого разъяснения наиболее существенных для организации политик безопасности, принципов, стандартов и требований соответствия, например:
e) определения общих и конкретных обязанностей сотрудников в рамках менеджмента информационной безопасности, включая информирование об инцидентах безопасности;
f) ссылок на документы, дополняющие политику информационной безопасности, например более детальные политики и процедуры безопасности для определенных информационных систем, а также правила безопасности, которым должны следовать пользователи.
1) соответствие законодательным требованиям и договорным обязательствам;
2) требования по обеспечению осведомленности, обучения и тренинга в отношении безопасности;
3) менеджмент непрерывности бизнеса;
4) ответственность за нарушения политики информационной безопасности;

Данная политика информационной безопасности должна быть доведена до сведения пользователей в рамках всей организации в актуальной, доступной и понятной форме.

Политика информационной безопасности может составлять часть документа по общей политике. Если политика информационной безопасности распространяется за пределами организации, следует принимать меры в отношении неразглашения чувствительной информации.

Пересмотр политики информационной безопасности

Политика информационной безопасности должна пересматриваться либо через запланированные интервалы времени, либо, если произошли значительные изменения, с целью обеспечения уверенности в ее актуальности, адекватности и эффективности.

Политика информационной безопасности должна иметь владельца, который утвержден руководством в качестве ответственного за разработку, пересмотр и оценку политики безопасности. Пересмотр заключается в оценке возможностей по улучшению политики информационной безопасности организации и подхода к менеджменту информационной безопасности в ответ на изменения организационной среды, обстоятельств бизнеса, правовых условий или технической среды.

При пересмотре политики информационной безопасности следует учитывать результаты пересмотров методов управления. Должны существовать определенные процедуры пересмотра методов управления, в том числе график или период пересмотра.

Входные данные для пересмотра методов управления должны включать информацию об:

a) ответной реакции заинтересованных сторон;

b) результатах независимых пересмотров;

c) состоянии предотвращающих и корректирующих действий;

d) результатах предыдущих пересмотров методов управления;

e) выполнении процесса и соответствии политике информационной безопасности;

f) изменениях, которые могли бы повлиять на подход организации к методам управления информационной безопасностью, включая изменения, касающиеся организационной среды, обстоятельств бизнеса, доступности ресурсов, контрактных, регулирующих и правовых условий или технической среды;

g) тенденциях в отношении угроз и уязвимостей;

h) доведенных до сведения инцидентах информационной безопасности ;

i) рекомендациях, данных соответствующими органами.

Выходные данные пересмотра методов управления должны включать любые решения и действия относительно:

a) улучшения подхода организации к менеджменту информационной безопасности и ее процессов;

b) улучшения мер и средств контроля и управления и целей их применения;

c) улучшения распределения ресурсов и (или) обязанностей.

Пересмотр методов управления следует документировать.

Пересмотренная политика должна быть утверждена руководством.

6. Организационные аспекты информационной безопасности

6.1 Задачи, решаемые внутри организации

Осуществлять менеджмент информационной безопасности в рамках организации.

Должна быть создана структура менеджмента для инициирования и контроля обеспечения информационной безопасности в организации

Высшее руководство должно утверждать политику информационной безопасности организации, назначать ответственных лиц в области политики информационной безопасности, а также координировать и анализировать внедрение информационной безопасности в организации

При необходимости следует предусмотреть наличие контактного лица, занимающегося вопросами информационной безопасности внутри организации, к которому могут обращаться заинтересованные сотрудники. Следует налаживать контакты с отдельными внешними специалистами по безопасности или группами специалистов, включая соответствующие органы, чтобы находиться в курсе отраслевых тенденций, осуществлять мониторинг стандартов и методов оценки, и обеспечивать адекватные точки контакта при обработке инцидентов информационной безопасности. Следует поощрять многопрофильный подход к обеспечению информационной безопасности.

6.1.1 Обязательства руководства по отношению к информационной безопасности

Мера и средство контроля и управления

Руководству следует активно поддерживать безопасность в организации с помощью четкого управления, видимого распределения обязанностей, определенных назначений и признания обязанностей в отношении информационной безопасности.

Руководству следует:

a) обеспечивать уверенность в том, что цели информационной безопасности определены, соответствуют требованиям организации и включены в соответствующие процессы;

b) формулировать, анализировать и утверждать политику информационной безопасности;

c) анализировать эффективность реализации политики информационной безопасности;

d) обеспечивать четкое управление и очевидную поддержку менеджмента в отношении инициатив, связанных с безопасностью;

e) обеспечивать ресурсы, необходимые для информационной безопасности;

f) утверждать определенные роли и ответственности в отношении информационной безопасности в рамках организации;

g) инициировать планы и программы для поддержки осведомленности об информационной безопасности;

h) обеспечивать уверенность в том, что реализация мер и средств контроля и управления информационной безопасности скоординирована в рамках организации

Руководству следует определять потребность в консультациях с внутренними или внешними специалистами по информационной безопасности, а также анализировать и координировать результаты консультаций в рамках организации.

В зависимости от величины организации такие обязанности могут выполняться специальным административным совещанием или существующим органом управления, например советом директоров.

6.1.2 Координация вопросов информационной безопасности

Мера и средство контроля и управления

Деятельность, связанная с информационной безопасностью, должна быть скоординирована представителями различных подразделений организации с соответствующими ролями и должностными обязанностями.

Рекомендация по реализации

Как правило, координация проблем информационной безопасности должна включать в себя сотрудничество и участие менеджеров, пользователей, администраторов, разработчиков прикладных программ, аудиторов и персонала, занимающегося безопасностью, а также специалистов в области страхования, правовых аспектов, кадровых ресурсов, ИТ или менеджмента риска.

Такая деятельность должна:

a) обеспечивать уверенность в том, что обеспечение безопасности осуществляется в соответствии с политикой информационной безопасности;

b) определять способ устранения несоответствия;

c) утверждать методики и процессы обеспечения информационной безопасности, например оценку риска, классификацию информации;

d) выявлять значительные изменения угроз и подверженность информации и средств обработки информации угрозам;

e) оценивать адекватность и координировать реализацию мер и средств контроля и управления информационной безопасности;

f) эффективно способствовать осведомленности, обучению и тренингу в отношении информационной безопасности в рамках организации;

g) оценивать информацию, полученную в результате мониторинга и анализа инцидентов информационной безопасности, и рекомендовать соответствующие действия в ответ на выявленные инциденты информационной безопасности.

3 Распределение обязанностей по обеспечению информационной безопасности

Все обязанности по обеспечению информационной безопасности должны быть четко определены.

Распределение обязанностей по обеспечению информационной безопасности следует осуществлять в соответствии с политикой информационной безопасности Следует четко определять обязанности по защите отдельных активов и по выполнению конкретных процессов, связанных с информационной безопасностью. Такие обязанности следует дополнять, при необходимости, более детальными руководствами для конкретных мест эксплуатации и средств обработки информации. Конкретные обязанности в отношении защиты активов и осуществления специфических процессов, связанных с безопасностью, например планирование непрерывности бизнеса, должны быть четко определены.

Лица, на которые возложена обязанность по обеспечению безопасности, могут делегировать задачи, связанные с безопасностью, другим лицам. Тем не менее, они остаются ответственными за выполнение делегированных задач.

Круг обязанностей каждого руководителя должен быть четко определен, в частности:

a) активы и процессы (процедуры) безопасности, связанные с каждой конкретной системой, должны быть четко определены;

b) необходимо назначить ответственных за каждый актив или процедуру безопасности, и подробно описать их обязанности в соответствующих документах (см. 7.1.2);

c) уровни полномочий должны быть четко определены и документально оформлены.

Дополнительная информация

Во многих организациях назначается менеджер по информационной безопасности, на которого возлагается общая ответственность за разработку и реализацию безопасности и за поддержку определения мер и средств контроля и управления.

Однако обязанности в отношении поиска ресурсов и реализации мер и средств контроля и управления часто вменяются отдельным менеджерам. Общепринятой практикой является назначение владельца для каждого актива, который несет ответственность за его повседневную защиту.

4 *Процесс получения разрешения на использование средств обработки информации*

Необходимо определить и реализовать процесс получения разрешения у руководства на использование новых средств обработки информации.

В отношении процесса получения разрешения следует рассмотреть следующие рекомендации:

a) на новые средства должны быть получены соответствующие разрешения руководства пользователей, утверждающего их цель и использование. Разрешение следует также получать от менеджера, ответственного за поддержку среды безопасности локальной информационной системы, чтобы обеспечить уверенность в том, что все соответствующие требования и политики безопасности соблюдаются;

b) аппаратные средства и программное обеспечение, где необходимо, следует проверять на предмет совместимости с другими компонентами системы;

c) использование персональных или находящихся в частной собственности средств обработки информации, например лэптопов, домашних компьютеров или карманных устройств для обработки деловой информации может являться причиной новых уязвимостей, поэтому следует определять и реализовывать необходимые меры и средства контроля и управления.

5 Соглашения о конфиденциальности

Требования в отношении соглашений о конфиденциальности или неразглашении, отражающие потребности организации в защите информации, должны определяться и регулярно пересматриваться.

В соглашениях о конфиденциальности или неразглашении должно содержаться требование о защите конфиденциальной информации, выраженное юридическими терминами, имеющими исковую силу.

Чтобы определить требования для соглашений о конфиденциальности или неразглашении, необходимо учесть следующие факторы:

a) определение информации, подлежащей защите (например конфиденциальная информация);

b) предполагаемый срок действия соглашения, включая случаи, когда может возникнуть необходимость в неограниченной поддержке конфиденциальности;

c) необходимые действия при окончании срока действия соглашения;

d) обязанности и действия лиц, подписавших соглашение, с целью предотвращения несанкционированного разглашения информации (например по принципу "необходимого знания");

e) владение информацией, коммерческие тайны и интеллектуальная собственность, и как это соотносится с защитой конфиденциальной информации;

f) разрешенное использование конфиденциальной информации и права лиц, подписавших соглашение, в отношении использования информации;

g) право подвергать аудиту и мониторингу деятельность, связанную с конфиденциальной информацией;

h) процедуру предупреждения и сообщения о несанкционированном разглашении или нарушениях, связанных с конфиденциальной информацией;

i) условия возврата или уничтожения информации в случае приостановления действия соглашения;

j) предполагаемые действия, которые должны быть предприняты в случае нарушения данного соглашения.

В зависимости от требований безопасности организации, могут потребоваться дополнительные элементы соглашения о конфиденциальности или неразглашении.

Соглашения о конфиденциальности и неразглашении должны соответствовать всем применимым законам и нормам, под юрисдикцию которых они подпадают

Требования в отношении соглашений о конфиденциальности и неразглашении должны пересматриваться периодически и когда происходят изменения, влияющие на эти требования.

Соглашения о конфиденциальности и неразглашении защищают информацию организации, а также информируют лиц, подписавших соглашение, об их обязанности защищать, использовать и разглашать информацию внушающим доверие и санкционированным способом.

При различных обстоятельствах организации могут потребоваться различные формы соглашений о конфиденциальности или неразглашении.

7 Контакт со специализированными профессиональными группами

Должны поддерживаться соответствующие контакты со специализированными профессиональными группами или участниками форумов по безопасности, а также с профессиональными ассоциациями.

Членство в специализированных группах или форумах следует рассматривать как средство для:

a) повышения знания о "передовом опыте" и достижений информационной безопасности на современном уровне;

b) обеспечения уверенности в том, что понимание проблем информационной безопасности является современным и полным;

c) получения раннего оповещения в виде предупреждений, информационных сообщений касающихся атак и уязвимостей;

d) возможности получения консультаций специалистов по вопросам информационной безопасности;
e) совместного использования и обмена информацией о новых технологиях, продуктах, угрозах или уязвимостях;
f) обеспечения адекватных точек контакта для обсуждения инцидентов информационной безопасности .

Могут быть установлены соглашения на совместное использование информации с целью улучшения сотрудничества и координации по вопросам безопасности. В таких соглашениях должны быть определены требования в отношении защиты чувствительной информации.

8 Независимая проверка информационной безопасности

Подход организации к менеджменту информационной безопасности и ее реализации (т.е. цели управления, политики, процессы и процедуры по обеспечению информационной безопасности) должен проверяться независимым образом через запланированные интервалы времени, или когда произошли значительные изменения, связанные с реализацией безопасности.

Независимая проверка должна инициироваться руководством. Такая независимая проверка необходима для обеспечения уверенности в сохраняющейся работоспособности, адекватности и эффективности подхода организации к менеджменту информационной безопасности. Проверка должна включать в себя оценку возможностей улучшения и необходимость изменений подхода к безопасности, в том числе политику и цели управления.

Такая проверка должна осуществляться специалистами, не работающими в рассматриваемой области деятельности, например службой внутреннего аудита, независимым менеджером или сторонней организацией, специализирующейся на таких проверках. Специалисты, привлекаемые к таким проверкам, должны обладать соответствующими навыками и опытом.

Результаты независимой проверки должны регистрироваться и сообщаться руководству, инициировавшему проверку. Эти отчеты необходимо сохранять для возможного последующего использования.

Если в результате независимой проверки устанавливается, что подход организации и реализация менеджмента информационной безопасности неадекватны или не соответствуют направлению информационной безопасности, изложенному в документе, содержащем политику информационной безопасности (см. 5.1.1), руководству следует рассмотреть соответствующие корректирующие действия.

Область деятельности, которую менеджеры должны регулярно проверять, может быть проверена независимым образом. Методы проверки могут включать опрос руководства, проверку данных регистрации или анализ документов, имеющих отношение к политике безопасности. ИСО 19011 [15] также может предоставить полезное руководство по выполнению независимой проверки, включая создание и реализацию программы проверки. В 15.3 определены меры и средства контроля и управления, имеющие значение для независимой проверки эксплуатируемых информационных систем и использования инструментальных средств аудита.