ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Информационная технология

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководство по внедрению системы управления информационной безопасностью

(ISO/IEC 27003:2010, MOD)

Издание официальное

Узбекское агентство стандартизации, метрологии и сертификации
Ташкент

Предисловие

1 РАЗРАБОТАН Государственным унитарным предприятием Центр научно-технических и маркетинговых исследований - «UNICON.UZ» (ГУП «UNICON.UZ»)

2 ВНЕСЕН Техническим комитетом по стандартизации в сфере связи и информатизации № 7

3 ПРИНЯТ Постановлением Узбекского агентства стандартизации, метрологии и сертификации от 19.06.2014 № 05-550

4 Настоящий стандарт модифицирован относительно международного стандарта ISO/IEC 27003:2010 Information technology - Security techniques - Information security management systems implementation guidance (ISO/IEC 27003:2010 Информационная технология. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью)

Сведения о соответствии ссылочных государственных стандартов Узбекистана международным стандартам приведены в дополнительном приложении G.

Информация о замене и дополнении ссылок в разделе 2 «Нормативные ссылки» с разъяснением причин их замены приведена в приложениях G, H.

Полный перечень технических отклонений с объяснением причин их внесения приведен в приложении H настоящего стандарта.

Перевод с английского языка (en).

Степень соответствия – модифицированная (MOD)

5 ВВЕДЕН ВПЕРВЫЕ

Содержание

Введение

Цель настоящего стандарта заключается в том, чтобы предоставить практическое руководство по разработке плана внедрения системы управления информационной безопасностью (СУИБ) для организаций в соответствии с требованиями и рекомендациями O‘z DSt ISO/IEC 27001. Фактически внедрение СУИБ обычно выполняется также как и внедрение проекта.

Процессы, описанные в настоящем стандарте, обеспечивают поддержку внедрения требований O‘z DSt ISO/IEC 27001, содержащихся в соответствующих пунктах разделов 4, 5 и 7, и документирования:

- подготовленного первоначального плана внедрения СУИБ в организации, определяющего организационную структуру проекта и получение разрешения руководства;
- плана обеспечения бесперебойной работы СУИБ;
- примеров успешного выполнения требований O‘z DSt ISO/IEC 27001.

С помощью настоящего стандарта организация сможет разработать процесс управления информационной безопасностью и предоставить заинтересованным сторонам гарантии того, что риски информационной безопасности для информационных активов будут постоянно поддерживаться в пределах допустимых границ, установленных организацией.

В настоящем стандарте не рассматриваются вопросы эксплуатации и других работ СУИБ, в нем рассматриваются только принципы деятельности по проектированию СУИБ, в результате которой будет получен окончательный план внедрения проекта СУИБ. Фактическая реализация специфической организационной части проекта СУИБ находится за пределами области рассмотрения настоящего стандарта.

При внедрении проекта СУИБ должны быть использованы стандартные методологии управления проектами, дополнительная информация о которых содержится в соответствующих стандартах в области управления проектами.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Ахборот технологияси

ХАВФСИЗЛИКНИ ТАЪМИНЛАШ УСУЛЛАРИ

Ахборот хавфсизлигини бошқариш тизимини жорий этиш бўйича қўлланма

Информационная технология

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Руководство по внедрению системы управления информационной безопасностью

Information technology
Security techniques
Information security management system implementation guidance

Дата введения 2014-06-23

1 Область применения

В настоящем стандарте рассматриваются важнейшие аспекты успешного проектирования и внедрения СУИБ в соответствии с требованиями O‘z DSt ISO/IEC 27001. В нем описан процесс формирования требований и проектирования СУИБ от начала проектирования и до разработки планов внедрения. Также описан процесс получения разрешения руководства на внедрение СУИБ, специфицирован проект внедрения СУИБ (далее - проект СУИБ), даются рекомендации по планированию проекта внедрения СУИБ, в результате чего будет получен окончательный план внедрения СУИБ.

Настоящий стандарт предназначен для использования организациями, внедряющими СУИБ. Он применим ко всем типам организаций (например, к коммерческим предприятиям, государственным органам, некоммерческим организациям) всех размеров. Структура и риски каждой организации уникальны, вследствие этого ее специфические требования оказывают влияние на внедрение СУИБ. Небольшие организации могут решить, что применимые к ним действия, описанные в настоящем стандарте, могут быть упрощены. Крупномасштабные или сложные организации могут решить, что многоуровневая организация или система управления нуждается в эффективном управлении действиями, определенными в настоящем стандарте. Однако в обоих случаях соответствующие действия могут быть запланированы с помощью настоящего стандарта.

Издание официальное

Настоящий стандарт не содержит каких-либо требований, а содержит только рекомендации и пояснения. Настоящий стандарт предполагается использовать совместно с базовыми стандартами СУИБ O‘z DSt ISO/IEC 27001 и O‘z DSt ISO/IEC 27002, его предназначением не является изменение и/или уменьшение требований, определенных в O‘z DSt ISO/IEC 27001, или рекомендаций, приведенных в O‘z DSt ISO/IEC 27002. Вследствие вышеизложенного настоящий стандарт не предназначен для использования при сертификации.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

O‘z DSt ISO 9001:2009 Системы менеджмента качества. Требования

O‘z DSt ISO 14001:2009 Государственная система стандартизации Республики Узбекистан. Система управления окружающей средой. Технические условия и руководство по применению

O‘z DSt ISO/IEC 27000:2014 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь

O‘z DSt ISO/IEC 27001:2009 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования

O‘z DSt ISO/IEC 27002:2008 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью

O‘z DSt ISO/IEC 27004:2014 Информационная технология. Методы обеспечения безопасности. Методы обеспечения безопасности. Измерение эффективности системы управления информационной безопасностью

O‘z DSt ISO/IEC 27005:2013 Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности

O‘z DSt ISO/IEC 27006:2013 Информационная технология. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью

3 Термины и определения

В настоящем стандарте применены термины по O‘z DSt ISO/IEC 27000, O‘z DSt ISO/IEC 27001, а также следующий термин с соответствующим определением:

3.1 **проект СУИБ:** Структурированные виды деятельности, предпринимаемые организацией при внедрении СУИБ.

4 Структура настоящего стандарта

4.1 Разделы стандарта

Внедрение СУИБ является особым видом деятельности организации и обычно выполняется как проект. Настоящий стандарт описывает процессы внедрения СУИБ, при этом особое внимание обращено на процессы инициации, планирования и определения проекта. Процесс окончательного планирования внедрения СУИБ подразделяется на пять следующих фаз, описанных в разных разделах, имеющих сходную структуру:

a) получение разрешения руководства на инициацию проекта СУИБ (раздел 5);

b) определение области действия и политики СУИБ (раздел 6);

c) проведение анализа организации (раздел 7);

d) выполнение оценки рисков и планирование их обработки (раздел 8);

e) проектирование СУИБ (раздел 9).

На рисунке 1 показаны пять фаз планирования проекта СУИБ и основные выходные документы.

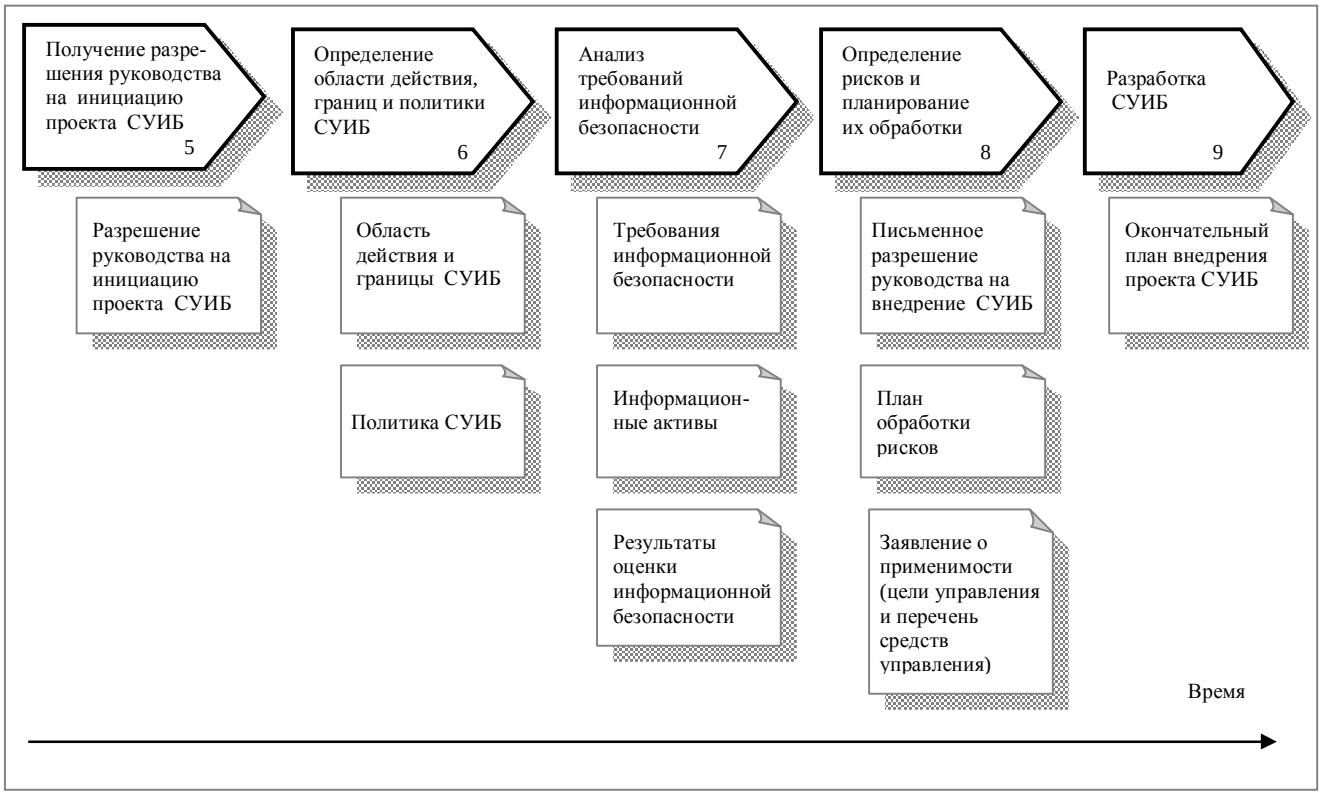


Рисунок 1 – Фазы проекта СУИБ

Дополнительная информация приведена в следующих приложениях:

- приложение A «Контрольная таблица»;
- приложение B «Распределение ролей и ответственности в области информационной безопасности»;
- приложение C «Внутренний аудит»;
- приложение D «Структура политик»;
- приложение E «Мониторинг и измерения»;
- приложение F «Примеры критических факторов успеха».

4.2 Структура разделов стандарта

Каждый раздел настоящего стандарта имеет следующую структуру:

a) в начале каждого раздела приводится одна или несколько поставленных целей, которые должны быть достигнуты, помещенные в рамку;

b) описывается один или несколько процессов, необходимых для достижения цели или целей фазы.

Каждый процесс описывается в отдельном подразделе. Описание процесса имеет следующую структуру:

Деятельность

Деятельность определяет, что необходимо для достижения всех или части целей фазы.

Входные данные

Входные данные описывают исходное состояние, например, наличие документированных решений или выходных данных других видов деятельности, описанных в настоящем стандарте. Входные данные также могут рассматриваться как выходные данные завершенной деятельности просто путем ссылки на соответствующий раздел или специфическую информацию о деятельности, добавленную после ссылки на раздел.

Рекомендации

Рекомендации содержат подробную информацию, необходимую для выполнения указанного вида деятельности. Некоторые рекомендации не являются универсальными для всех случаев, поэтому для достижения необходимых результатов могут быть использованы другие более подходящие методы.

Выходные данные

Выходные данные описывают результат(ы) завершенного вида деятельности или предоставляемый материал, например, документ. Выходные данные едины для всех организаций, независимо от их размера или области действия СУИБ.

Дополнительная информация

Дополнительная информация может содержать любую информацию, которая может быть полезна при выполнении деятельности, например, ссылки на другие стандарты.

Примечание - В настоящем стандарте в описаниях фаз и видов деятельности приведена примерная последовательность выполнения деятельности, основанная на взаимозависимостях, установленных с помощью описаний «входных» и «выходных» данных каждой деятельности. Тем не менее, в зависимости от многих различных факторов (например, от эффективности существующей системы управления, понимания значимости информационной безопасности, причины внедрения СУИБ), организация может при подготовке к разработке и внедрению СУИБ (при необходимости) выбрать любой вид деятельности в любой последовательности.

4.3 Схемы

Для получения общего представления о видах деятельности и выходных данных проект часто иллюстрируется графиками или схемами.

На рисунке 2 показаны условные обозначения на схемах, которые иллюстрируют краткие обзоры всех фаз проекта. Схемы обеспечивают повышение наглядности краткого обзора деятельности каждой фазы.

В верхнем прямоугольнике показаны планируемые фазы проекта СУИБ. Фаза, пояснения к которой содержатся в соответствующем разделе, обозначена своими ключевыми выходными документами.

На нижней схеме (деятельность фазы) показаны основные виды деятельности, которые соответствуют выделенной фазе верхнего прямоугольника, и основные выходные документы каждой деятельности.

Ось времени нижнего прямоугольника основана на оси времени верхнего прямоугольника.

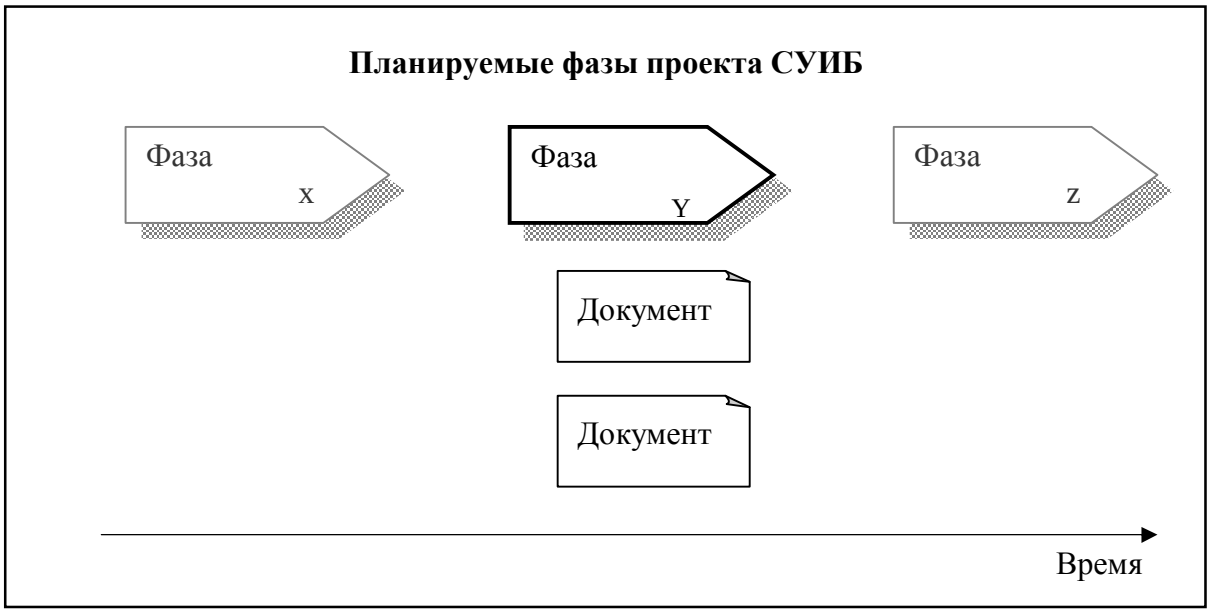
Деятельность А и деятельность В могут выполняться одновременно. Деятельность С должна начинаться после завершения деятельностей А и В.

5 Получение разрешения руководства на инициацию проекта СУИБ

5.1 Введение

Существует несколько факторов, которые должны быть учтены при принятии решения о внедрении СУИБ. Для того, чтобы рассмотреть эти факторы, высшее руководство организации должно основательно ознакомиться с экономическим обоснованием проекта внедрения СУИБ и одобрить его. Следовательно, целью данной фазы является:

Цель: Получение разрешения руководства на начало проектирования СУИБ, разработку экономического обоснования и плана проекта.



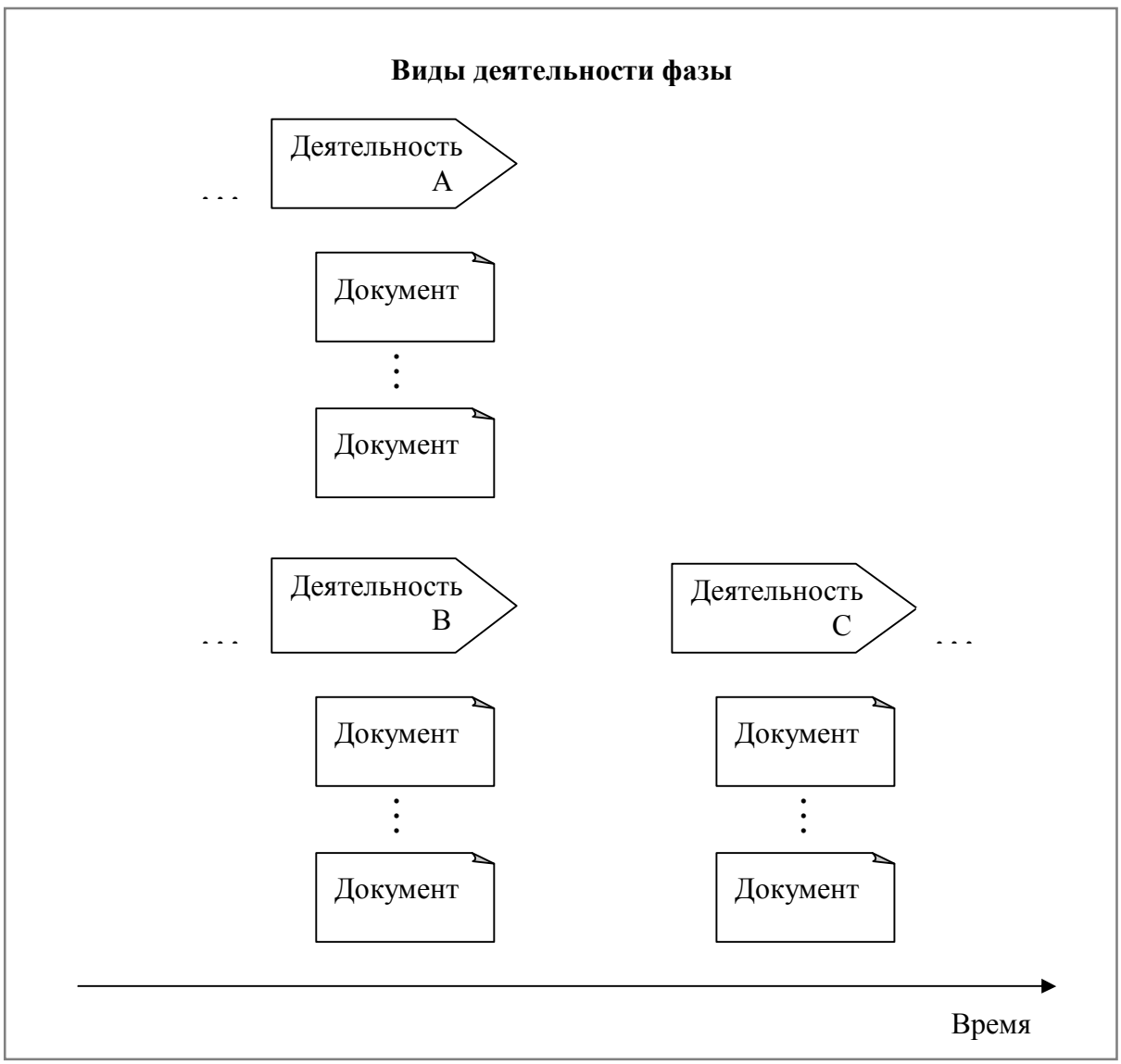


Рисунок 2 – Условные обозначения на схемах

Для получения разрешения руководства организация должна разработать экономическое обоснование, которое в дополнение к организационной структуре СУИБ включает приоритеты и цели внедрения СУИБ, а также предварительный план проекта СУИБ.

Выполнение работ этой фазы позволит организации осознать значимость СУИБ, уточнить роли и ответственность в области информационной безопасности персонала организации, необходимые при проектировании СУИБ.

Предполагаемыми выходными данными этой фазы будет получение предварительного разешения, приверженность руководства внедрению СУИБ и выполнению тех видов деятельности, которые описаны в настоящем стандарте. Также должны быть предоставлены следующие материалы: экономическое обоснование и черновой вариант плана проекта СУИБ, разбитый на основные этапы.

На рисунке 3 показан процесс получения разрешения руководства на инициацию проекта СУИБ.

Примечание - Стандарт O‘z DSt ISO/IEC 27001 не содержит требований к выходным данным раздела 5 (документированная приверженность руководства вопросам планирования и внедрения СУИБ) и к одним из выходных данных раздела 7 (документ, резюмирующий статус информационной безопасности). Тем не менее, выходные данные этих видов деятельности являются рекомендованными входными данными других видов деятельности, описанных в настоящем стандарте.

5.2 Определение приоритетов организации при разработке СУИБ

Деятельность

Включение приоритетов и требований информационной безопасности в цели внедрения СУИБ для рассматриваемой организации.

Входные данные

a) стратегические цели организации;

b) краткий обзор существующих систем управления;

c) перечень требований информационной безопасности, содержащихся в нормативно-правовых актах, договорах, применимых к организации.

Рекомендации

До начала проектирования СУИБ обычно необходимо получить разрешение руководства. Следовательно, первым видом деятельности, которая должна быть выполнена, будет являться сбор необходимой информации относительно стоимости СУИБ организации. Организация должна уточнить, зачем ей необходима СУИБ, и определить цели внедрения и инициации проекта СУИБ.

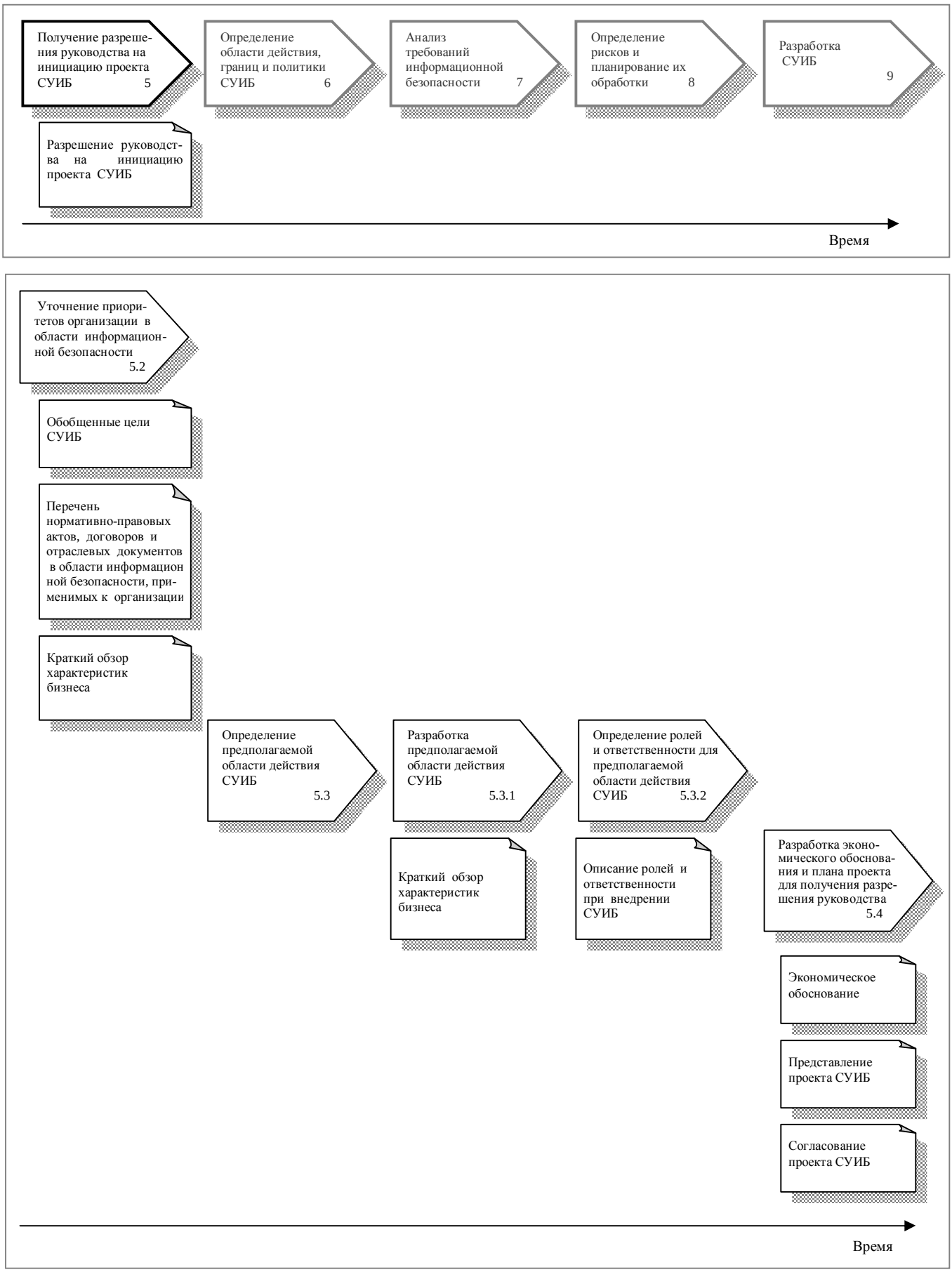


Рисунок 3 - Получение разрешения руководства на инициацию проекта СУИБ

Цели внедрения СУИБ могут быть определены при получении ответов на следующие вопросы:

a) управление рисками. Насколько СУИБ улучшит управление рисками информационной безопасности?

b) эффективность. Насколько СУИБ сможет улучшить управление информационной безопасностью?

c) преимущество для бизнеса. Насколько СУИБ сможет повысить конкурентоспособность организации?

Для получения ответов на вышеперечисленные вопросы необходимо определить приоритеты и требования организации в области информационной безопасности с учетом следующих факторов:

a) стратегически важные хозяйствующие субъекты и структурные подразделения:

1) какие хозяйствующие субъекты и структурные подразделения являются стратегически важными?

2) какие структурные подразделения обеспечивают деятельность организации и какие виды деятельности являются основными?

3) какие взаимоотношения и соглашения имеются с третьими сторонами?

4) существуют ли какие-либо внутренние процессы или производственные функции, переданные на аутсорсинг внешним организациям?

b) чувствительная или важная информация:

1) какая информация является для организации критической?

2) какие предположительно будут последствия, если определенная информация будет раскрыта сторонами, не имеющими на то соответствующих полномочий (например, потеря конкурентного преимущества, ущерб имиджу брэнда или репутации, судебный процесс и т.п.)?

c) нормативно-правовые акты в области информационной безопасности:

1) какие нормативно-правовые акты в области обработки рисков или информационной безопасности применимы к организации?

2) является ли организация частью международной глобальной организации, которой организация обязана предоставлять внешнюю финансовую отчетность?

d) договоры или организационные соглашения относительно информационной безопасности:

1) какие существуют требования к хранению данных (в том числе и к срокам хранения)?

2) имеются ли в договорах какие-либо требования относительно защиты персональных данных или качества (например, соглашение об уровне предоставления услуги)?

e) отраслевые требования, в которых определены конкретные меры или средства управления информационной безопасностью:

1) какие отраслевые требования применимы к организации?

f) угрозы для окружающей среды:

1) какая необходима защита и от каких угроз?

2) какие категории информации нуждаются в защите?

3) какие виды информационной деятельности должны быть защищены?

g) факторы конкурентоспособности:

1) какие существуют минимальные требования к информационной безопасности?

2) какие дополнительные средства управления информационной безопасностью будут способствовать конкурентоспособности организации?

h) требования непрерывности бизнеса:

1) что такое критические бизнес-процессы?

2) на какой срок организация может приостанавливать выполнение каждого критического бизнес-процесса?

Предполагаемая область действия СУИБ должна быть определена в результате анализа вышеприведенной информации, которая также будет необходима при разработке экономического обоснования и при согласовании руководством общего плана проекта СУИБ. Окончательно область действия СУИБ будет определена во время проектирования СУИБ.

Согласно 4.2.1, перечисление a) O‘z DSt ISO/IEC 27001 при определении области действия СУИБ необходимо учитывать характеристики бизнеса, организации, ее размещения, активов и технологий.

На начальном этапе принятия решений относительно области действия СУИБ должны быть рассмотрены следующие вопросы:

a) какие полномочия в области управления информационной безопасностью установлены руководством организации и какие внешние обязательства возложены на организацию?

b) будут ли нести ответственность за предполагаемую область действия системы несколько групп управления (например, сотрудники различных филиалов или отделов)?

c) каким образом документы СУИБ будут рассылаться по всей организации (например, в виде брошюр или посредством корпоративной сети)?

d) соответствует ли действующая система управления потребностям организации? Полностью ли она задействована, находится ли в хорошем состоянии и функционирует ли по предназначению?

Например, в перечень целей управления, которые могут быть использованы в качестве входов при определении предполагаемой области действия СУИБ, могут быть включены следующие цели:

a) обеспечение непрерывности бизнеса и восстановления работоспособности после возникновения отказов и сбоев;

b) повышение устойчивости к инцидентам;

c) выполнение требований нормативно-правовых актов, договорных условий или обязательств;

d) возможность сертификации на соответствие другим стандартам O‘z DSt ISO/IEC;

e) возможность реорганизации организации и изменения ее местоположения;

f) снижение расходов на средства управления безопасностью;

g) защита стратегически важных активов;

h) создание безопасной и эффективной внутренней среды управления;

i) предоставление заинтересованным сторонам гарантий того, что информационные активы защищены должным образом.

Выходные данные

В результате этой деятельности будут получены:

a) документ, обобщающий цели, приоритеты в области информационной безопасности и требования организации к СУИБ;

b) перечень нормативно-правовых актов, договоров и отраслевых документов, содержащих требования в области информационной безопасности и применимых к организации;

c) описание характеристик бизнеса, организации, ее размещения, активов и технологий.

Дополнительная информация

Дополнительная информация содержится в стандартах O‘z DSt ISO 9001, O‘z DSt ISO 14001.

5.3 Определение предполагаемой области действия СУИБ

5.3.1 Разработка предполагаемой области действия СУИБ

Деятельность

Цели внедрения СУИБ должны включать определение предполагаемой области действия СУИБ, которая необходима для проекта СУИБ.

Входные данные

Выход деятельности 5.2 «Определение приоритетов организации при разработке СУИБ».

Рекомендации

При разработке проекта внедрения СУИБ должна быть определена структура организации, для которой разрабатывается этот проект. Одновременно с этим должна быть определена предполагаемая область действия СУИБ. Все это позволит выдать руководству организации рекомендации по реализации решений и поддержке дальнейшей деятельности.

Предполагаемая область действия СУИБ необходима при разработке экономического обоснования и при получении разрешения руководства на использование предложенного плана проекта.

По завершению этого этапа будет получен документ, определяющий предполагаемую область действия СУИБ, который включает:

a) краткое изложение полномочий в области управления информационной безопасностью, устанавливаемых руководством организации, и внешних обязательств, возложенных на организацию;

b) описание взаимодействия сферы (сфер) деятельности, указанных в области действия, с другими системами управления;

c) перечень бизнес-целей в области управления информационной безопасностью (полученный согласно 5.2);

d) перечень критических бизнес-процессов, систем, информационных активов, зданий/помещений организации с указанием их географического местоположения, в которых будет использоваться СУИБ;

e) взаимосвязь существующих систем управления, нормативных актов, соответствующих стандартов и целей организации;

f) характеристики бизнеса, организации, ее размещения, активов и технологий.

Должны быть определены общие элементы и операционные различия между процессами любой существующей системы управления и предполагаемой СУИБ.

Выходные данные

Документ, в котором описана предполагаемая область действия СУИБ.

Дополнительная информация

Дополнительная информация отсутствует.

Примечание - При проведении сертификации необходимо обратить особое внимание на то, чтобы документация, относящаяся к области действия СУИБ, соответствовала требованиям O‘z DSt ISO/IEC 27001 к документации, независимо от существующих в организации систем управления.

5.3.2 Определение ролей и ответственности для предполагаемой области действия СУИБ

Деятельность

Для предполагаемой области действия СУИБ должны быть определены все роли и ответственность.

Входные данные

a) выход деятельности, описанной в 5.3.1 «Разработка предполагаемой области действия СУИБ»;

b) перечень заинтересованных сторон, которые получат выгоду от результатов проектирования СУИБ.

Рекомендации

При проектировании СУИБ среди персонала организации должны быть распределены роли в области информационной безопасности. Обычно роли в каждой организации распределяются по-разному, это зависит от количества сотрудников, занимающихся деятельностью в области обеспечения информационной безопасности. Организационная структура и ресурсы в области информационной безопасности изменяются в зависимости от размера, типа и структуры организации. Например, в маленькой организации одним и тем же сотрудником могут выполняться несколько ролей. Тем не менее, руководство должно однозначно определить роль с полной ответственностью за управление информационной безопасностью (обычно это руководитель отдела информационной безопасности, администратор информационной безопасности или т.п.); распределение ролей и ответственности среди сотрудников должно производиться с учетом их квалификации, необходимой для выполнения этой работы. Это является очень важным фактором, необходимым для обеспечения эффективного и результативного выполнения задач.

Наиболее важными при определении ролей в области управления информационной безопасностью являются следующие аспекты:

a) общая ответственность за выполнение задач лежит на руководстве;

b) ответственным за координацию процесса обеспечения информационной безопасности назначается одно лицо (обычно руководитель отдела обеспечения информационной безопасности);

c) каждый сотрудник в равной степени ответственен за свою основную задачу и за поддержание информационной безопасности на своем рабочем месте и в организации.

Роли в области управления информационной безопасностью должны взаимодействовать; эту задачу можно облегчить с помощью рабочей группы по информационной безопасности или другого аналогичного органа.

На всех этапах разработки, внедрения, функционирования и эксплуатации СУИБ должно осуществляться (и документироваться) взаимодействие с соответствующими специалистами организации.

Представители подразделений в определенной области (например, в области управления рисками) являются потенциальными участниками рабочей группы по внедрению СУИБ. Эта рабочая группа должна быть постоянной, состоять из оптимального количества участников, обеспечивающих быстрое и эффективное использование ресурсов. Область действия СУИБ включает не только области, непосредственно касающиеся ее, но также косвенно включает такие подразделения, как например,

юридический и административные отделы, а также отдел управления рисками.

Выходные данные

Документ или таблица, содержащие наименования ролей и описания их ответственности, необходимые для успешного внедрения СУИБ в организации.

Дополнительная информация

Дополнительная информация приведена в приложении В, в котором подробно описаны роли и их ответственность, необходимые для успешного внедрения СУИБ в организации.

5.4 Разработка экономического обоснования, плана проекта и получение разрешения руководства

Деятельность

Представление разработанного экономического обоснования и проекта СУИБ руководству, получение разрешения руководства и обязательства выделения ресурсов, необходимых для внедрения проекта СУИБ.

Входные данные

a) выходные данные деятельности 5.2 «Определение приоритетов организации при разработке СУИБ»;

b) выходные данные деятельности 5.3 «Определение предполагаемой области действия СУИБ» - задокументированные предполагаемые:

1) область действия СУИБ;

2) взаимосвязь ролей и ответственности.

Рекомендации

Информация, необходимая для разработки экономического обоснования и инициации плана проекта СУИБ, должна включать примерный график работ, ресурсы и этапы основной деятельности, описанные в разделах 6 и 9 настоящего стандарта.

Экономическое обоснование и инициация плана проекта СУИБ служат не только основой проекта, но также и основой для обеспечения приверженности руководства и обоснования выделения ресурсов, необходимых для внедрения СУИБ. Таким образом внедрение СУИБ будет способствовать достижению бизнес-целей, эффективности организационных процессов и повышению результативности бизнеса.

Экономическое обоснование внедрения СУИБ должно состоять из кратких формулировок, связанных с целями организации, и отражать следующие аспекты:

a) задачи и специфические цели;

b) преимущества для организации;

c) предполагаемая область действия СУИБ, включая наиболее затрагиваемые бизнес-процессы;

d) критические процессы и факторы, необходимые для достижения целей СУИБ;

e) краткий обзор высшего уровня проекта;

f) предварительный план внедрения;

g) определение ролей и ответственности;

h) необходимые ресурсы (технология, персонал);

i) соображения относительно внедрения с учетом существующей системы обеспечения информационной безопасности;

j) график работ с разбивкой по основным этапам;

k) ожидаемые затраты;

l) критические факторы успеха;

m) расчет экономического эффекта для организации.

План проекта должен включать соответствующие деятельности фаз, описанные в разделах с 6 по 9 настоящего стандарта.

Должны быть определены лица, которые будут участвовать во внедрении СУИБ, и те лица, чьи интересы будут затронуты СУИБ; им должно быть выделено необходимое время для ознакомления с экономическим обоснованием и проектом СУИБ, а также для написания соответствующих замечаний и предложений. По мере поступления вышеуказанных замечаний и предложений экономическое обоснование и предлагаемый проект СУИБ должны корректироваться (при необходимости). При получении всех согласований экономическое обоснование и предлагаемый проект СУИБ должны быть представлены руководству на утверждение.

Руководство должно утвердить экономическое обоснование и план инициируемого проекта для достижения полной приверженности организации и начала реализации проекта СУИБ.

Ожидаемыми преимуществами от приверженности руководства к внедрению СУИБ являются:

a) знание и применение соответствующих нормативно-правовых актов, договорных обязательств и стандартов в области информационной безопасности, это позволит избежать ответственности и наказания за их несоблюдение;

b) эффективное использование многократных процессов обеспечения информационной безопасности;

c) увеличение стабильности и укрепление доверия за счет лучшего управления рисками информационной безопасности;

d) идентификация и защита критической бизнес-информации.

Выходные данные

Результатами этой деятельности являются:

a) документированное разрешение руководства на внедрение проекта СУИБ и выделение ресурсов;

b) документированное экономическое обоснование;

c) предлагаемый проект инициируемой СУИБ с разбивкой по этапам (например, определение рисков, внедрение, внутренний аудит и анализ со стороны руководства).

Дополнительная информация

Примеры критических факторов успеха, необходимых для поддержки экономического обоснования СУИБ, приведены в приложении F.

6 Определение области действия, границ и политики СУИБ

6.1 Введение

Разрешение руководства на внедрение СУИБ основывается на предполагаемой области действия СУИБ, экономическом обосновании СУИБ и плане инициируемого проекта. Детальное определение области действия и границ СУИБ, определение политики СУИБ, согласование и поддержка руководством являются первичными ключевыми факторами успешного внедрения СУИБ.

Следовательно, целями этой фазы являются:

Цели: Детальное определение области действия и границ СУИБ, разработка политики СУИБ, получение согласования у руководства. Ссылки: 4.2.1, перечисления a), b) O‘z DSt ISO/IEC 27001

Для достижения цели «Детальное определение области действия и границ СУИБ» необходимо определить следующее:

- область действия и границы организации;
- область действия и границы информационно-коммуникационных технологий (ИКТ);
- физические область действия и границы;
- согласно 4.2.1, перечисления a), b) O‘z DSt ISO/IEC 27001 характеристики бизнеса, организации, ее размещения, аспекты области действия и границ активов и технологий; в процессе определения этих областей действия и границ определится политика СУИБ;
- совокупные область действия и границы СУИБ путем объединения всех вышеуказанных областей действия и границ.

Следующим действием будет являться разработка политики СУИБ и ее согласование с руководством.

Для создания эффективной СУИБ организации должна быть детально определена ее область действия с учетом особо важных для организации информационных активов. Настоятельно рекомендуется при идентификации информационных активов и оценке работоспособности механизмов безопасности использовать общепринятую терминологию и системный подход. Это существенно облегчит взаимопонимание и будет способствовать лучшему пониманию всей последовательности фаз внедрения СУИБ. Также необходимо обеспечить включение в ее область действия наиболее важных подразделений организации.

Возможно, что определенная область действия СУИБ будет распространяться на всю организацию или ее часть, например, подразделение или четко ограниченное подразделение ее филиала. Например, в случае предоставления «услуг» потребителям область действия СУИБ может распространяться на службу или многофункциональную систему управления (целое подразделение или его часть). При сертификации СУИБ требования O‘z DSt ISO/IEC 27001 должны быть обязательно выполнены независимо от существующих систем управления конкретной организации.

Определение области действия и границ организации, области действия и границ ИКТ (6.3), физических области действия и границ (6.4) не всегда должны выполняться в указанной последовательности. Тем не менее, при определении других областей действия и границ будет нелишне ссылаться на уже полученные области действия и границы.

Определение области действия, границ и политики СУИБ показано на рисунке 4.

6.2 Определение области действия и границ организации

Деятельность

Определение области действия и границ организации.

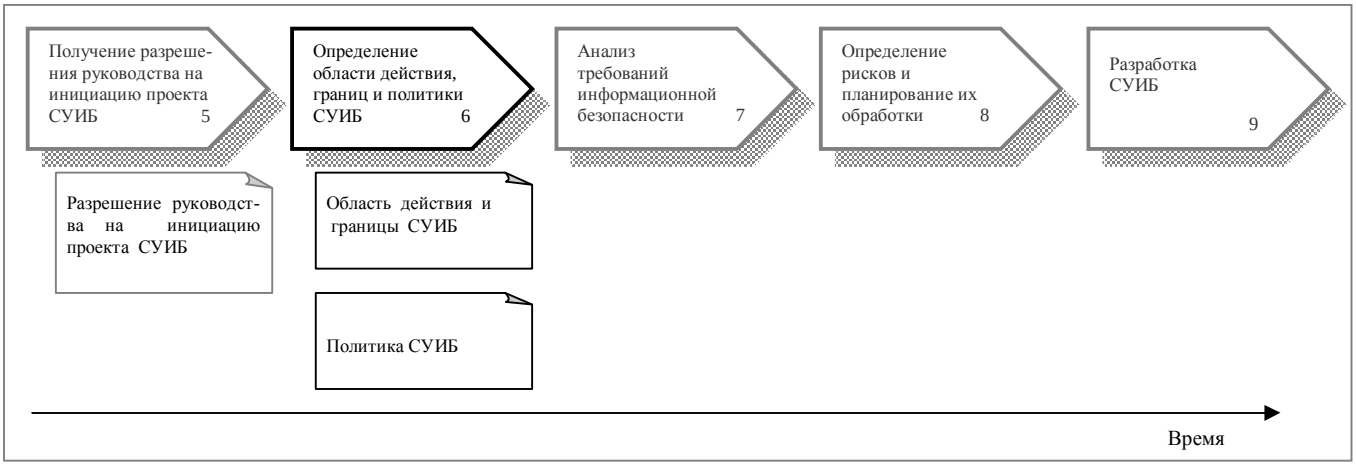
Входные данные

a) выходные данные деятельности 5.3 «Определение предполагаемой области действия СУИБ» - документ, с описанием предполагаемой области действия СУИБ, в котором рассматриваются:

1) взаимосвязь существующих систем управления, нормативно-правовых актов, соответствующих стандартов и целей организации;

2) характеристики бизнеса, организации, ее размещения, активов и технологий;

b) выходные данные деятельности 5.2 «Определение приоритетов организации при разработке СУИБ» - документированное разрешение руководства на внедрение СУИБ, запуск проекта и выделение необходимых ресурсов.



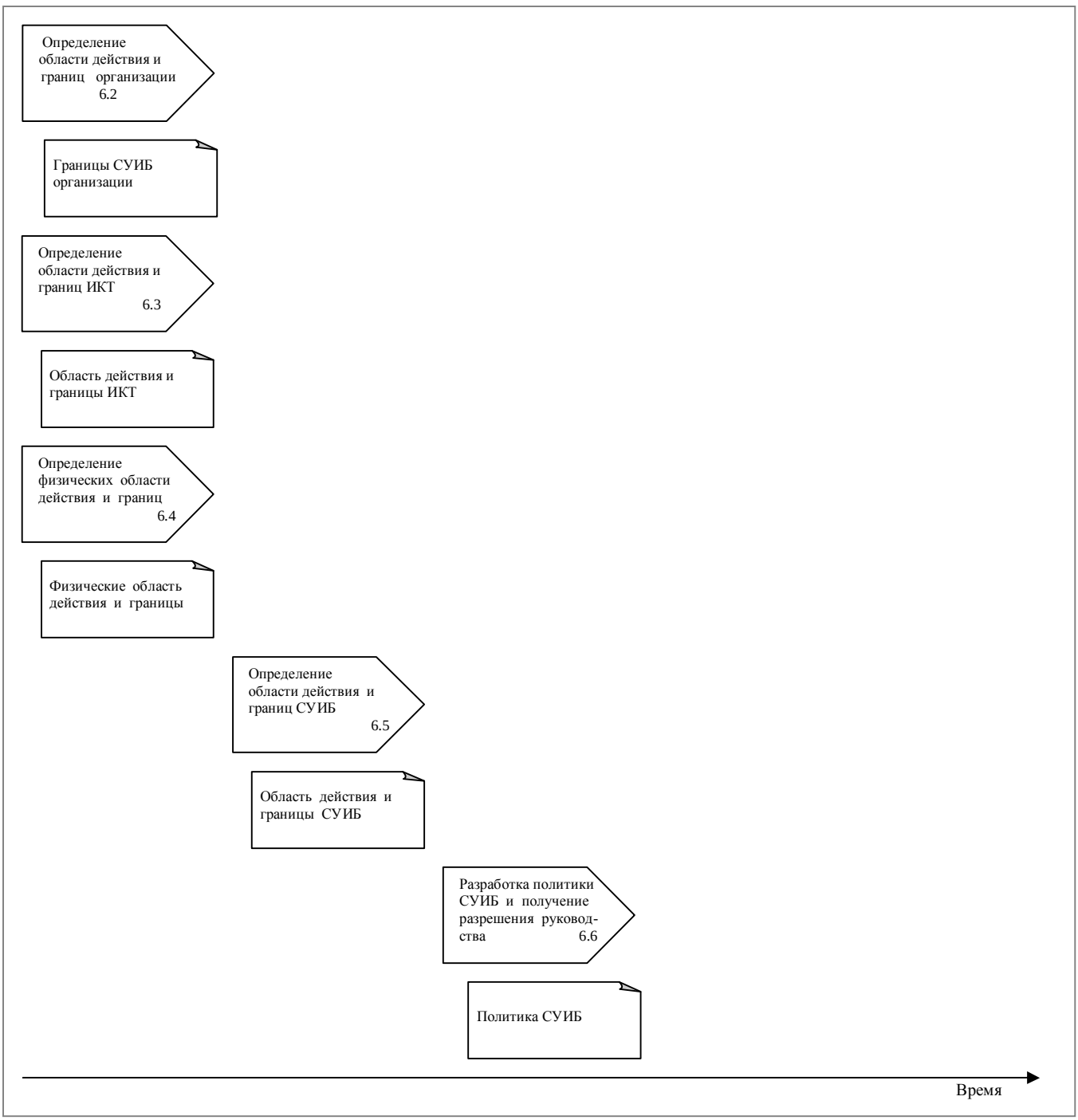


Рисунок 4 - Определение области действия, границ и политики СУИБ

Рекомендации

Количество усилий, необходимых для внедрения СУИБ зависит от величины области действия, в которой она будет применяться. Это также может повлиять на всю деятельность, связанную с обеспечением в этой области действия информационной безопасности объектов (например, процесс, физическое месторасположение, информационные системы и персонал), включая внедрение и эксплуатацию средств управления, управление операциями, а также выполнение таких задач, как идентификация информационных активов и определение рисков.

Если руководство примет решение об исключении определенных частей организации из области действия СУИБ, то причины этого решения должны быть задокументированы.

При определении области действия СУИБ очень важно, чтобы ее границы были определены достаточно четко, чтобы сотрудникам, не участвовавшим в их определении, можно было легко объяснить, где проходят эти границы.

Возможно, что некоторые средства управления информационной безопасностью уже используются в других системах управления. Они должны быть учтены при планировании СУИБ, но границы области действия действующей СУИБ указывать не обязательно.

Один из методов определения границ организации заключается в идентификации непересекающихся сфер ответственности, это облегчит распределение в организации подотчетности.

Сферы ответственности, непосредственно связанные с информационными активами или бизнес-процессами, входящими в область действия СУИБ, должны быть выбраны как часть организации, которая находится под управлением СУИБ. При определении границ организации должны быть учтены следующие факторы:

a) рабочая группа по управлению СУИБ должна состоять из администраторов, непосредственно вовлеченных в область действия СУИБ;

b) представителем руководства, ответственным за СУИБ, должно быть то лицо, которое, в конечном счете, ответственно за все сферы затронутых обязанностей (то есть его роль, как правило, диктуется его зоной контроля и ответственности в пределах организации);

c) в том случае, когда роль ответственного за СУИБ определена лицу, не входящему в состав высшего руководства, то в составе высшего руководства должно быть определено лицо, занимающееся вопросами информационной безопасности и обеспечивающее поддержку СУИБ на верхних уровнях организации;

d) правильное определение области действия и границ гарантирует, что при определении рисков были учтены все соответствующие активы и что риски, которые могут проникнуть через эти границы, рассмотрены.

При анализе границ организации, основанном на этом методе, должны быть идентифицированы все сотрудники организации, подвергающиеся воздействию СУИБ, которые должны быть включены в ее область

действия. Идентификация персонала может быть связана с процессами и/или функциями в зависимости от выбранного метода. Если некоторые процессы в пределах области действия выполняются сторонними организациями, то эти взаимоотношения должны быть четко документированы. Эти взаимоотношения будут впоследствии проанализированы при внедрении проекта СУИБ.

Выходные данные

Результатами этой деятельности являются:

a) описание границ организации для СУИБ, включающее обоснования исключений из области действия СУИБ каких-либо частей организации;

b) функции и структура частей организации в пределах области действия СУИБ;

c) определение информации, обмен которой происходит в пределах области действия СУИБ, и информации, обмен которой происходит через границы;

d) процессы, происходящие в организации, и ответственность за информационные активы, находящиеся в пределах области действия СУИБ и за ее пределами;

e) иерархический процесс принятия решений, а также иерархическая структура в пределах СУИБ.

Дополнительная информация

Дополнительная информация отсутствует.

6.3 Определение области действия и границ ИКТ

Деятельность

Определение области действия и границ элементов ИКТ и элементов других технологий, используемых СУИБ.

Входные данные

a) выходные данные деятельности 5.3 «Определение предполагаемой области действия СУИБ» - документ, содержащий описание предполагаемой области действия СУИБ;

b) выходные данные деятельности 6.2 «Определение области действия и границ организации».

Рекомендации

Область действия и границы ИКТ могут быть определены методом, используемым для информационной системы (вместо метода, используемого для информационных технологий). После того, как руководством было принято решение о включении бизнес-процессов информационной системы в область действия СУИБ, также должны быть учтены все

связанные с ней элементы ИКТ. Они включают в себя все те части организации, которые хранят, обрабатывают или транспортируют критическую информацию, активы или которые являются критическими для других частей организации в области действия. Действие информационных систем может быть ограничено как границами организации, так и границами государства. В любом случае необходимо учитывать следующие факторы:

a) социально-культурную среду;

b) применимые к организации требования, содержащиеся в нормативно-правовых актах и договорах;

c) подотчетность в основных сферах ответственности;

d) технические ограничения (например, доступная пропускная способность, доступность услуги и т.п.)

С учетом вышеизложенного описание границ ИКТ, где это применимо, должно содержать следующие сведения:

a) инфраструктура связи, в которой используются различные технологии (например, проводные и беспроводные сети или сети передачи данных/телефонные сети), ответственность за управление которой возложена на организацию;

b) программное обеспечение, используемое и контролируемое организацией;

c) аппаратные средства ИКТ, необходимые для сети или сетей, приложений или производственных систем;

d) роли и ответственность относительно аппаратных средств ИКТ, сети и программного обеспечения.

Если какой-либо один или несколько из вышеуказанных пунктов не контролируется организацией, зависимость от третьей стороны должна быть задокументирована согласно 6.2.

Выходные данные

Результатами этой деятельности являются:

a) информация, обмен которой происходит в пределах области действия СУИБ, и информация, обмен которой происходит через границы;

b) границы ИКТ для СУИБ, включая обоснования исключения ИКТ, которыми управляет организация, из области действия СУИБ;

c) описание информационных систем и сетей телекоммуникаций, входящих в область действия, а также распределение ролей и ответственности для этих систем. Системы, находящиеся вне области действия, должны быть кратко описаны.

Дополнительная информация

Дополнительная информация отсутствует.

6.4 Определение физических области действия и границ

Деятельность

Определение физических области действия и границ СУИБ.

Входные данные

a) выходные данные деятельности 5.3 «Определение предполагаемой области действия СУИБ» - документ, содержащий описание предполагаемой области действия СУИБ;

b) выходные данные деятельности 6.2 «Определение области действия и границ организации»;

c) выходные данные деятельности 6.3 «Определение области действия и границ ИКТ».

Рекомендации

Определение физических области действия и границ заключается в определении зданий, помещений или оборудования организации, которые должны стать частью СУИБ. Гораздо сложнее это сделать для распределенных информационных систем, которые пересекают физические границы организации и для которых необходимы:

a) периферийное оборудование;

b) пользовательские интерфейсы информационных систем и услуги, предоставляемые службами третьей стороны;

c) применение соответствующих интерфейсов и уровней обслуживания.

С учетом вышеизложенного описание физических границ, где это применимо, должно включать следующее:

a) описание функций или процессов и средств управления с учетом их физического местоположения в организации;

b) специальное оборудование, используемое для хранения/размещения аппаратных средств ИКТ или данных области действия (например, резервные копии на магнитных носителях), расположенное в границах ИКТ.

Если какой-либо один или несколько из вышеуказанных пунктов не контролируется организацией, зависимость от третьей стороны должна быть задокументирована согласно 6.2.

Выходные данные

Результатами этой деятельности являются:

a) описание физических границ СУИБ с обоснованиями исключения из области действия СУИБ некоторых физических границ организации;

b) описание организации и ее географических характеристик относительно области действия СУИБ.

Дополнительная информация

Дополнительная информация отсутствует.

6.5 Определение области действия и границ СУИБ

Деятельность

Получение области действия и границ СУИБ путем объединения всех областей действия и границ.

Входные данные

a) выходные данные деятельности 5.3 «Определение предполагаемой области действия СУИБ» - документ, содержащий описание предполагаемой области действия СУИБ;

b) выходные данные деятельности 6.2 «Определение области действия и границ организации»;

c) выходные данные деятельности 6.3 «Определение области действия и границ ИКТ»;

d) выходные данные деятельности 6.4 «Определение физических области действия и границ».

Рекомендации

Область действия СУИБ может быть описана и обоснована многими способами. Например, используя физическое местоположение выбранного центра обработки/хранения данных или офиса, можно будет перечислить те критические процессы, которые протекают за его пределами. Область действия этих процессов следует включить в область действия СУИБ. Одним из таких критических процессов может быть, например, доступ к центральной информационной системе мобильных пользователей.

Выходные данные

Результатом этой деятельности является документ, описывающий область действия и границы СУИБ и содержащий следующую информацию:

a) основные характеристики организации (ее функции, структура, службы, активы, область действия и границы ответственности для каждого актива);

b) процессы организации в области действия СУИБ;

c) конфигурация оборудования и сетей в области действия СУИБ;

d) предварительный список информационных активов в области действия СУИБ;

e) список активов ИКТ (например, серверов) в области действия СУИБ;

f) схемы расположения объектов, определяющие физические границы СУИБ;

g) описание ролей и ответственности в пределах СУИБ и их взаимосвязь со структурой организации;

h) детальное описание и обоснование всех исключений из области действия СУИБ.

Дополнительная информация

Дополнительная информация отсутствует.

6.6 Разработка политики СУИБ и получение разрешения руководства

Деятельность

Разработка политики СУИБ и получение разрешения руководства.

Входные данные

a) выходные данные деятельности 6.5 «Определение области действия и границ СУИБ» - документ, содержащий описание области действия и границ СУИБ;

b) выходные данные деятельности 5.2 «Определение приоритетов организации при разработке СУИБ» - документ, описывающий цели внедрения СУИБ;

c) выходные данные деятельности 5.4 «Разработка экономического обоснования, плана проекта и получение разрешения руководства» - документы:

1) требования и приоритеты организации в области информационной безопасности;

2) первоначальный план проекта внедрения СУИБ с разбивкой по этапам (например, определение рисков, внедрение, внутренний аудит и анализ со стороны руководства).

Рекомендации

При определении политики СУИБ должны быть учтены следующие аспекты:

a) установленные цели СУИБ, основанные на требованиях и приоритетах организации в области информационной безопасности;

b) установленные общий приоритет и руководство к действию по достижению целей СУИБ;

c) учитываемые требования организации, нормативно-правовых актов и договоров в области информационной безопасности;

d) состояние управления рисками в пределах организации;

e) установленные критерии оценки рисков и структура определения рисков;

f) уточненная ответственность руководства высшего уровня относительно СУИБ;

g) полученное разрешение руководства.

Выходные данные

Результатом этой деятельности является документ, описывающий утвержденную руководством политику СУИБ. Этот документ должен быть повторно утвержден в последующей фазе проекта, поскольку он зависит от результатов определения риска.

Дополнительная информация

Дополнительная информация относительно критериев оценки рисков содержится в O‘z DSt ISO/IEC 27005.

7 Анализ требований информационной безопасности

7.1 Введение

Анализ текущей ситуации в организации очень важен, так как при внедрении СУИБ должны быть учтены существующие требования и информационные активы. Те виды деятельности, которые описаны в этой фазе, из соображений эффективности и практичности могут выполняться большей частью параллельно с видами деятельности, описанными в разделе 6.

Цели:

Определение требований для соответствующей СУИБ, идентификация информационных активов и получение данных о текущем состоянии информационной безопасности в пределах области действия СУИБ.

Ссылки: 4.2.1, перечисление c) 1) частично; 4.2.1, перечисления d), e) O‘z DSt ISO/IEC 27001

В информации, собранной в процессе анализа информационной безопасности организации, должно содержаться следующее:

a) данные об исходном состоянии, предоставляемые руководству (то есть правильные основные данные);

b) выявленные и задокументированные условия внедрения;

c) четкое и хорошо обоснованное понимание функциональных возможностей организации;

d) принимаемые во внимание конкретные обстоятельства и ситуация в организации;

e) необходимый уровень защиты информации;

f) распоряжение относительно сбора и обобщения информации, необходимой для всей организации или ее части в пределах предполагаемой области действия СУИБ.

Выполнение анализа требований информационной безопасности показано на рисунке 5.

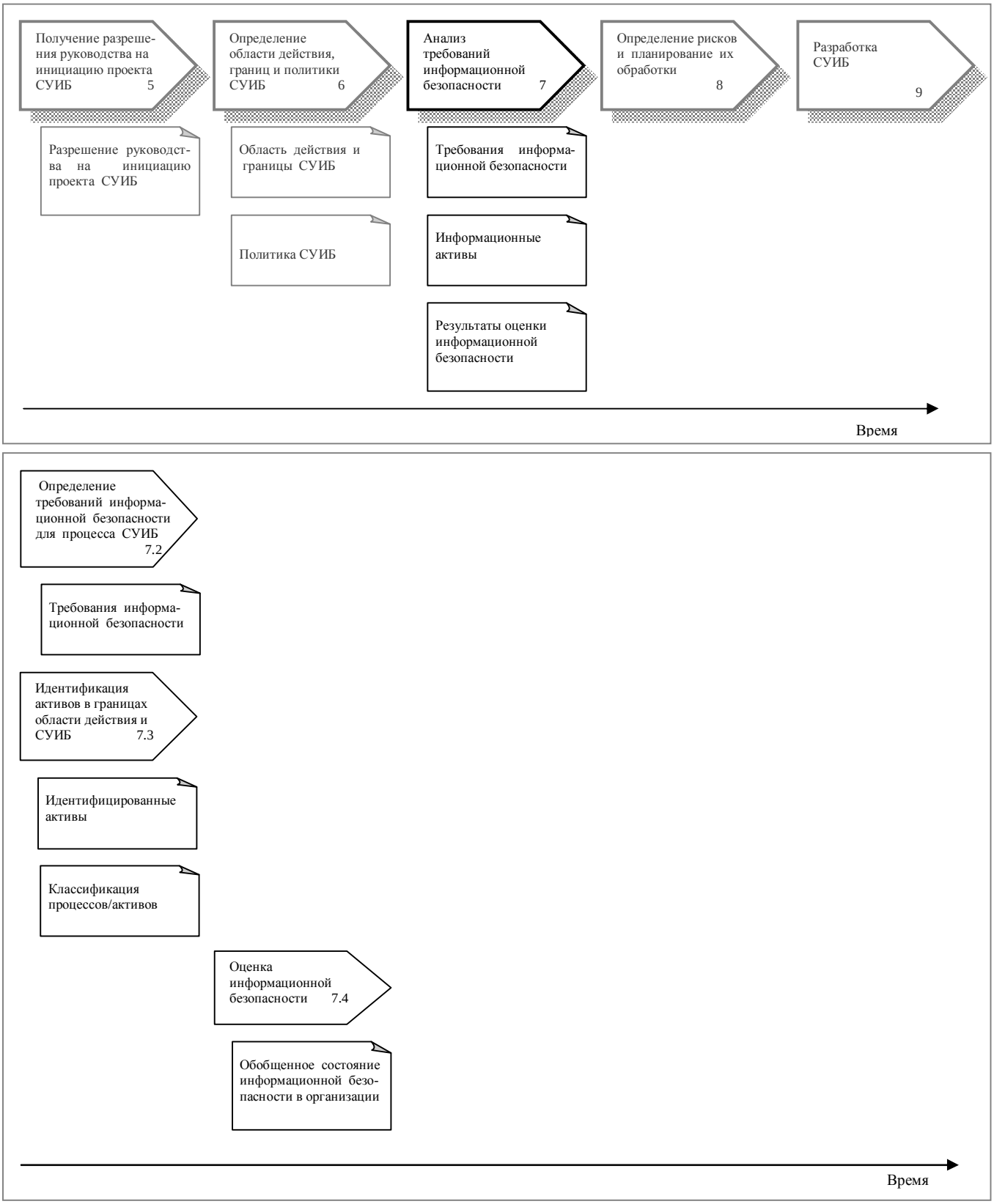


Рисунок 5 – Анализ требований информационной безопасности

7.2 Определение требований информационной безопасности для процесса СУИБ

Деятельность

Анализ и определение детализированных требований информационной безопасности для процесса СУИБ.

Входные данные

a) выходные данные деятельности 5.2 «Определение приоритетов организации при разработке СУИБ» - документы:

1) краткое изложение целей, приоритетов организации в области информационной безопасности и требований организации к СУИБ;

2) список нормативно-правовых, договорных и отраслевых ограничений в области информационной безопасности организации;

b) выходные данные деятельности 6.5 «Определение области действия и границ СУИБ» - область действия и границы СУИБ;

c) выходные данные деятельности 6.6 «Разработка политики СУИБ и получение разрешения руководства» - политика СУИБ.

Рекомендации

Вначале для СУИБ необходимо собрать всю дополнительную информацию. Для каждого процесса и специализированной задачи организации должно быть принято решение относительно защиты критической информации, то есть относительно требуемого уровня защиты. Необходимо определить то множество внутренних условий, которое может влиять на информационную безопасность. На этом этапе не требуется подробное описание информационной технологии. Основой отчета будет являться информация, полученная в результате анализа процесса организации и взаимосвязанных с ним приложений ИКТ и систем.

В результате анализа процессов организации будет получена информация о влиянии инцидентов информационной безопасности на деятельность организации. Во многих случаях для работы с базовым описанием процессов организации этого будет достаточно.

Если процессы, функции, местоположения, информационные системы и сети коммуникаций не были включены в область действия СУИБ, то они должны быть идентифицированы и задокументированы.

При определении детализированных требований информационной безопасности для СУИБ должно быть выполнено следующее:

a) предварительная идентификация важных информационных активов и определение существующего на данный момент уровня защиты информации;

b) определение видения организации и определение влияния этого видения на будущие требования к обработке информации;

c) анализ существующих форм обработки информации, системного программного обеспечения, сетей коммуникаций, местоположения деятельности, информационных ресурсов и т.п.;

d) определение всех основных требований (например, требований нормативно-правовых актов, договорных обязательств, требований организации и отраслевых стандартов, контрактов между заказчиком и поставщиком, условий страхования и т.п.);

e) определение уровня осведомленности в области информационной безопасности и, исходя из этого, определение требований к тренингам и обучению персонала каждого структурного и административного подразделения организации.

Выходные данные

Результатами этой деятельности являются:

a) идентификация основных процессов, функций, местоположений, информационных систем и сетей телекоммуникаций;

b) информационные активы организации;

c) классификация критических процессов/активов;

d) требования информационной безопасности, полученные из требований нормативно-правовых актов, а также из требований договоров организации;

e) перечень общеизвестных уязвимостей, которые должны быть учтены при определении требований информационной безопасности;

f) требования к тренингам и обучению персонала организации в области информационной безопасности.

Дополнительная информация

Дополнительная информация отсутствует.

7.3 Идентификация активов в пределах области действия СУИБ

Деятельность

Идентификация активов, которые должны поддерживаться СУИБ.

Входные данные

a) выходные данные деятельности 6.5 «Определение области действия и границ СУИБ» - область действия и границы СУИБ;

b) выходные данные деятельности 6.6 «Разработка политики СУИБ и получение разрешения руководства» - политика СУИБ;

c) выходные данные деятельности 7.2 «Определение требований информационной безопасности для процесса СУИБ».

Рекомендации

Для идентификации активов в пределах области действия СУИБ должна быть определена и перечислена следующая информация:

a) уникальное имя процесса;

b) описание процесса и взаимосвязанных с ним действий (создание, хранение, передача, удаление);

c) критичность процесса для организации (критический, важный, вспомогательный);

d) владелец процесса (подразделение организации);

e) процессы, обеспечивающие входные и выходные данные этого процесса;

f) приложения для информационных технологий, поддерживающие процесс;

g) классификация информации (конфиденциальность, целостность, доступность, управление доступом, неотказуемость и/или ее другие важные для организации свойства, например, время хранения информации).

Выходные данные

Результатами этой деятельности являются:

a) идентификация информационных активов основных процессов организации в пределах области действия СУИБ;

b) классификация критических процессов и информационных активов относительно характеристик информационной безопасности.

Дополнительная информация

Дополнительная информация отсутствует.

7.4 Оценка информационной безопасности

Деятельность

Оценка информационной безопасности путем сравнения текущего состояния информационной безопасности в организации с намеченными целями организации.

Входные данные

a) выходные данные деятельности 6.5 «Определение области действия и границ СУИБ» - область действия и границы СУИБ;

b) выходные данные деятельности 6.6 «Разработка политики СУИБ и получение разрешения руководства» - политика СУИБ;

c) выходные данные деятельности 7.2 «Определение требований информационной безопасности для процесса СУИБ»;

d) выходные данные деятельности 7.3 «Идентификация активов в пределах области действия СУИБ».

Рекомендации

Оценка информационной безопасности - это деятельность по определению существующего уровня информационной безопасности (то есть используемых в организации при обработке информации процедур защиты). Основная цель оценки информационной безопасности заключается в предоставлении дополнительной информации для описания, необходимого для системы управления, в виде политики и рекомендаций. Конечно, необходимо убедиться в том, что все выявленные недостатки устраняются одновременно согласно плану приоритетных действий. Все участвующие в оценке информационной безопасности организации стороны должны быть ознакомлены с результатами анализа состояния информационной безопасности, стандартами и нормативными документами, и иметь доступ к соответствующему руководящему персоналу.

При проведении оценки информационной безопасности выполняется анализ ее текущего состояния в организации, при этом используется нижеследующая информация, устанавливается текущее состояние информационной безопасности и уязвимости в документах:

a) изучение имевших место событий относительно критических процессов;

b) классификация информационных активов;

c) требования информационной безопасности организации.

Совокупность результатов оценки информационной безопасности и целей организации является важной частью мотивации предстоящей работы в области информационной безопасности. Оценка информационной безопасности должна выполняться внутренним или внешним независимым персоналом.

К проведению оценки информационной безопасности должны быть привлечены лица, которые хорошо осведомлены о существующей среде и условиях и которые могут влиять на информационную безопасность. В состав группы этих лиц должны быть выбраны представители всех подразделений организации, в том числе:

a) руководители структурных подразделений;

b) ответственные за процессы (то есть представители основных подразделений организации);

c) другие лица, которые хорошо осведомлены о существующей среде и условиях и которые могут влиять на информационную безопасность. Например, пользователи бизнес-процессов, а также персонал, выполняющий оперативные, административные и юридические функции.

Для успешного выполнения оценки информационной безопасности имеют важное значение следующие действия:

a) определение и составление перечня соответствующих стандартов организации (например, O‘z DSt ISO/IEC 27002);

b) определение общеизвестных требований к управлению, которые устанавливаются политиками, нормативно-правовыми актами, договорными обязательствами, результатами предыдущих аудитов или ранее выполненных определений рисков;

c) использование вышеуказанных документов в качестве справочных для приблизительной оценки соответствия уровня информационной безопасности организации установленным требованиям.

Определение приоритетов, выполненное в период анализа организации, представляет собой основу, для которой должны быть предусмотрены предупреждающие меры безопасности и контрольные устройства (средства управления).

Для проведения оценки информационной безопасности используется следующий метод:

a) выбрать основные бизнес-процессы организации и этапы процесса относительно требований информационной безопасности;

b) составить подробную блок-схему, охватывающую основные процессы организации, включая инфраструктуру (логическую и техническую), если это еще не было сделано в период анализа организации;

c) обсудить и проанализировать с соответствующими ведущими специалистами текущее состояние организации относительно требований информационной безопасности. Например, какие процессы являются критическими, насколько хорошо они в настоящее время работают? (Полученные результаты впоследствии будут использованы при определении рисков);

d) определить недостатки управления путем сравнения существующих средств управления с ранее определенными требованиями к управлению;

e) оформить и задокументировать текущее состояние.

Выходные данные

Результатом этой деятельности является документ, обобщающий существующее состояние безопасности в организации и обнаруженные уязвимости.

Дополнительная информация

В результате выполнения на данном этапе оценки информационной безопасности будет предоставлена только предварительная информация о состоянии информационной безопасности в организации и об уязвимостях, поскольку полный набор политик информационной безопасности и стандартов разрабатывается на последующем этапе (в соответствии с разделом 9), и определение рисков не было еще проведено.

8 Определение рисков и планирование их обработки

8.1 Введение

При внедрении СУИБ должны быть учтены основные риски информационной безопасности. Определение (рисунок 6), оценка и планирование обработки рисков, а также выбор целей управления и средств управления являются основными этапами внедрения СУИБ, рассматриваемые в данной фазе.

Специальные рекомендации по управлению рисками информационной безопасности, содержащиеся в O‘z DSt ISO/IEC 27005, будут рассмотрены также и в этом разделе.

Предполагается, что руководством уже было принято решение о внедрении СУИБ, область действия и политика СУИБ определены, а также известны информационные фонды и результаты оценки информационной безопасности.

Цель:

Определение методологии определения рисков, идентификация, анализ и оценка рисков информационной безопасности для выбора вариантов обработки рисков, выбор целей и средств управления.

Ссылки: 4.2.1, перечисления c) - j) O‘z DSt ISO/IEC 27001

8.2 Определение рисков

Деятельность

Выполнение определения рисков.

Входные данные

a) выходные данные деятельности раздела 7 «Анализ требований информационной безопасности» - информация относительно:

1) общего состояния информационной безопасности;

2) идентифицированных информационных активов;

b) выходные данные деятельности раздела 6 «Определение области действия, границ и политики СУИБ» - документы:

1) область действия СУИБ;

2) политика СУИБ;

c) O‘z DSt ISO/IEC 27005.

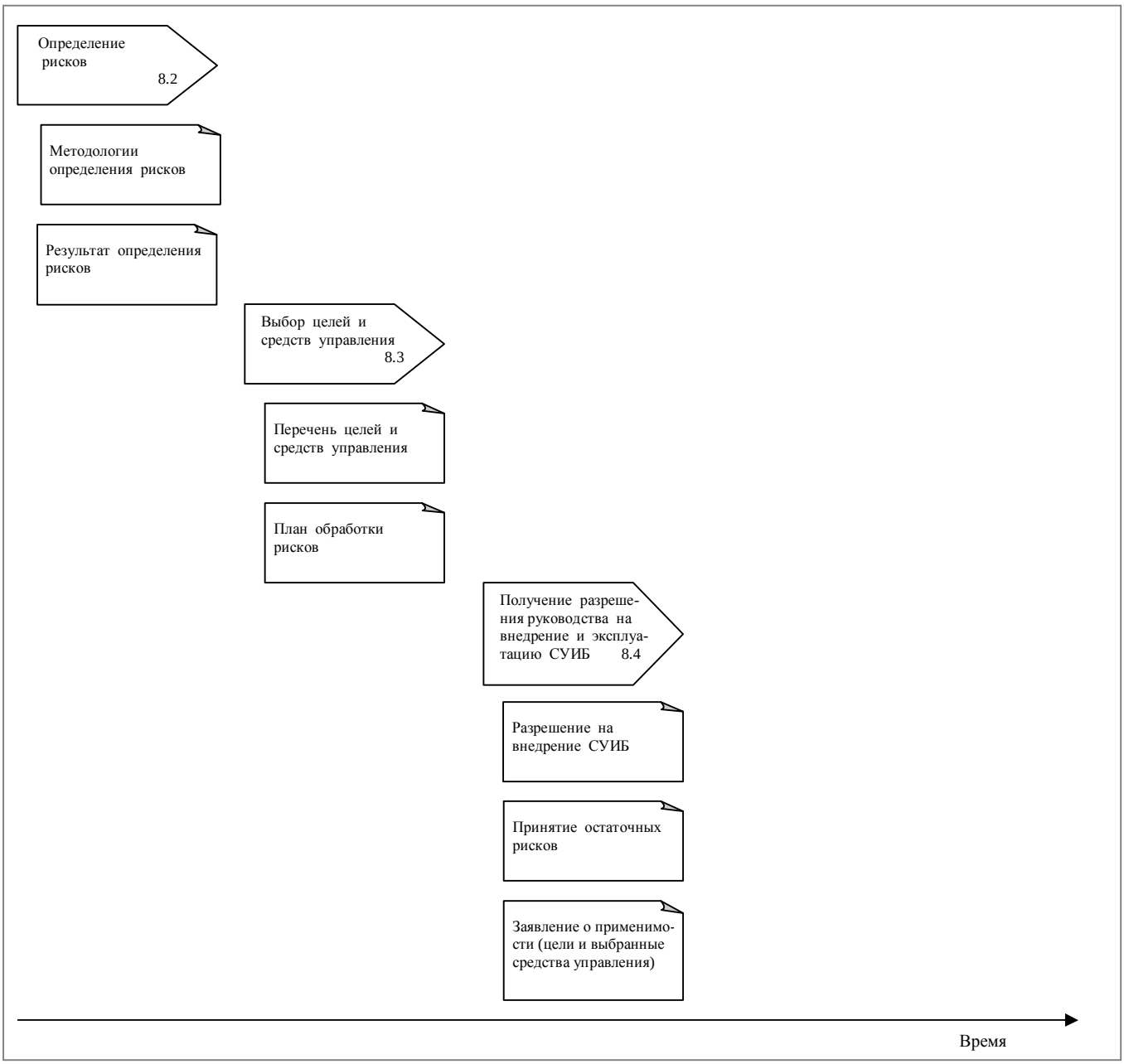


Рисунок 6 – Определение рисков

Определение рисков безопасности в контексте бизнес-деятельности организации для подтверждения области действия СУИБ является основой успешного внедрения СУИБ в соответствии с требованиями стандарта O‘z DSt ISO/IEC 27001. При определении рисков должны быть выполнены:

a) идентификация угроз и их источников;

b) идентификация существующих и планируемых средств управления;

c) идентификация уязвимостей, которые могут быть использованы при реализации угроз для нанесения ущерба активам или организации;

d) определение последствий нарушения конфиденциальности, целостности, доступности, неотказуемости и других требований по безопасности к активам;

e) оценка влияния на бизнес предполагаемых или имевших место инцидентов информационной безопасности;

f) оценка вероятных сценариев инцидентов;

g) предварительная оценка уровней рисков;

h) сравнение уровней рисков с критериями оценки рисков и критериями допустимых (приемлемых) рисков.

В определении рисков должны принимать участие лица, хорошо осведомленные о целях организации и обладающие знаниями в области безопасности (например, хорошо разбирающиеся в том, какие угрозы в настоящее время являются актуальными для целей организации). В состав группы этих лиц должны входить представители всех подразделений организации.

Организация может воспользоваться методологией определения рисков, предлагаемой конкретной компанией или содержащейся в конкретных проектах, или в соответствующем отраслевом стандарте.

Выходные данные

Результатами этой деятельности являются:

a) описание методологий определения риска;

b) результаты определения риска.

Дополнительная информация

Дополнительная информация содержится в приложении В «Распределение ролей и ответственности в области информационной безопасности».

Примечание – Сценарий инцидента – это описание угрозы, для реализации которой во время инцидента информационной безопасности используется одна определенная уязвимость или набор уязвимостей. Встречающиеся сценарии инцидентов, например «нарушение безопасности», описаны в O‘z DSt ISO/IEC 27001 и O‘z DSt ISO/IEC 27005

8.3 Выбор целей и средств управления

Деятельность

Определение вариантов обработки рисков, а также выбор средств управления, соответствующих определенным вариантам обработки рисков.

Входные данные

a) выходные данные деятельности 8.2 «Определение рисков» - результат определения рисков;

b) O‘z DSt ISO/IEC 27005;

c) O‘z DSt ISO/IEC 27002.

Рекомендации

Важно определить взаимосвязь между рисками и выбранными вариантами их обработки (например, план обработки рисков), так как от этого будет зависеть результат обработки рисков. Возможные варианты обработки рисков приведены в 4.2.1, перечисление f) O‘z DSt ISO/IEC 27001. Обязательное приложение A O‘z DSt ISO/IEC 27001 «Цели и средства управления» используется при выборе целей и средств управления обработки рисков. Если в приложении A соответствующие цели или средства управления отсутствуют, то должны быть определены и использованы дополнительные цели и средства управления. Необходимо продемонстрировать как выбранные средства управления в соответствии с требованиями плана обработки риска позволят снизить риски.

Данные, приведенные в приложении A O‘z DSt ISO/IEC 27001, не являются исчерпывающими. Для поддержки конкретных требований бизнеса, также как и СУИБ, могут быть определены специфические средства управления.

Установление взаимосвязей между каждым риском и выбранными целями и средствами управления в процессе снижения рисков будет полезно при разработке и внедрении СУИБ. Эти взаимосвязи можно добавить в список взаимосвязей между рисками и выбранными вариантами обработки рисков.

Для облегчения проведения аудита организация должна составить перечень выбранных для применения в СУИБ средств управления. Это придаст дополнительное преимущество при совершенствовании бизнес-отношений, например, предоставление отчета об установленных средствах управления с помощью электронного аутсорсинга.

Важно осознавать, что отчет об установленных средствах управления, весьма вероятно, будет содержать чувствительную информацию. Следовательно, при написании этого отчета необходимо учесть, что доступ к нему будут иметь как собственные сотрудники организации, так и сотрудники сторонних организаций. Возможно, что при определении активов будет целесообразно использовать информацию, полученную в ходе создания СУИБ.

Выходные данные

Результатами этой деятельности являются:

a) перечень выбранных целей и средств управления;

b) план обработки рисков, в том числе с описанием взаимосвязей между рисками и выбранными:

1) вариантами их обработки;

2) целями и средствами управления (особенно в случае снижения риска).

Дополнительная информация

Дополнительная информация приведена в O‘z DSt ISO/IEC 27002.

8.4 Получение разрешения руководства на внедрение и функционирование СУИБ

Деятельность

Получение разрешения руководства на внедрение СУИБ, а также документирование принятия остаточных рисков.

Входные данные

a) выходные данные деятельности 5.4 «Разработка экономического обоснования, плана проекта и получение разрешения руководства» - предварительное разрешение руководства на проект СУИБ;

b) выходные данные деятельности раздела 6 «Определение области действия, границ и политики СУИБ» - задокументированные:

1) политика и цели СУИБ;

2) область действия СУИБ;

c) выходные данные деятельности 8.2 «Определение рисков» - задокументированные:

1) описание методологий определения риска;

2) результат определения рисков;

d) выходные данные деятельности 8.3 «Выбор целей и средств управления» - план обработки рисков.

Рекомендации

Для получения разрешения руководства должны быть подготовлены и представлены руководству для рассмотрения и принятия решения вышеперечисленные документы.

Составление заявления о применимости должно быть включено в программу работ по управлению информационной безопасностью. Уровень детализации средств управления должен быть достаточным для поддержки разрешения руководства организации на внедрение СУИБ.

От руководства высшего уровня должны быть получены разрешение на принятие остаточных рисков и разрешение на фактическое функционирование СУИБ. Это разрешение должно быть основано на определении

рисков и вероятности их возникновения при внедрении СУИБ и при ее отсутствии.

Выходные данные

Результатами этой деятельности являются:

a) письменное разрешение руководства на внедрение СУИБ;

b) принятие руководством остаточных рисков;

c) заявление о применимости, включая цели и выбранные средства управления.

Дополнительная информация

Дополнительная информация отсутствует.

9 Разработка СУИБ

9.1 Введение

На этом этапе должны быть разработаны рабочая документация проекта СУИБ и план по его внедрению. Окончательный план проекта СУИБ будет уникально детализированным для конкретной организации в зависимости от результатов предыдущих деятельностей, а также результатов разработки, описанной в этом разделе.

Выходными данными этого раздела будет являться конкретный окончательный план внедрения проекта СУИБ. Проект СУИБ, основанный на этом плане, может быть запущен в организации как часть самой первой фазы «осуществление» цикла модели «планирование - осуществление – проверка – действие» [«Plan-Do-Check-Act» (PDCA)], описанной в O‘z DSt ISO/IEC 27001.

Предполагается, что приверженность руководства организации внедрению СУИБ оговорена в области действия и политике СУИБ. Также предполагается, что доступны информационные активы и результаты оценки информационной безопасности. Также должен быть доступен план обработки рисков, в котором описаны риски, варианты обработки рисков с идентифицированными выбранными целями и средствами управления.

Разработка СУИБ (рисунок 7), описываемая в данном разделе, сфокусирована на внутренней структуре и требованиях СУИБ. Необходимо отметить, что в определенных случаях разработка СУИБ может прямо или косвенно влиять на разработку бизнес-процессов. Также следует отметить, что обычно существует необходимость интеграции компонентов СУИБ с изначально существующими структурой и инфраструктурой управления.

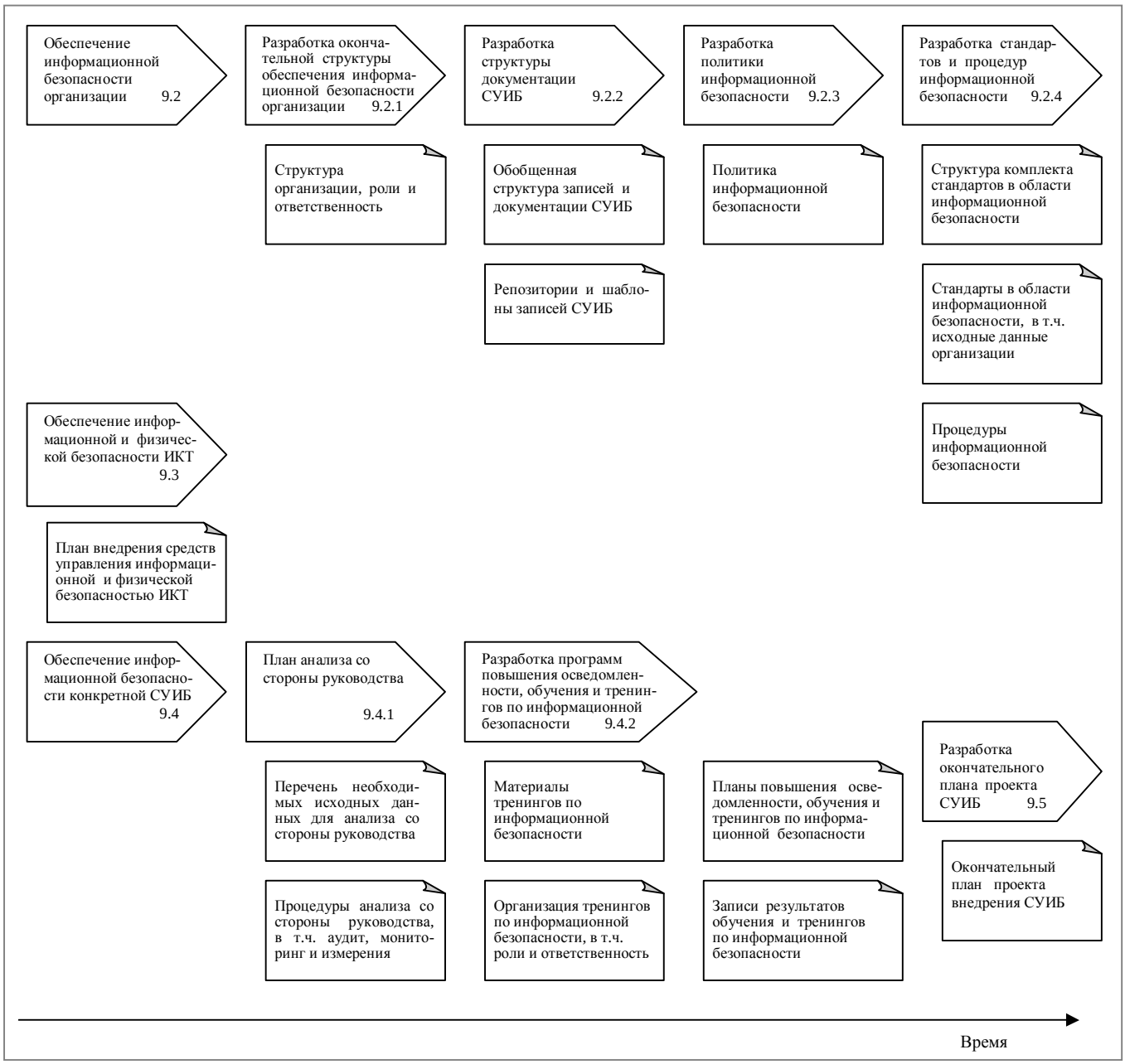


Рисунок 7 - Разработка СУИБ

Цель:

Завершение окончательного плана внедрения СУИБ: разработка безопасности организации на основе выбранных вариантов обработки рисков, а также требований по ведению записей и документированию, разработка комплексных средств управления, обеспечивающих защиту ИКТ, физических и организационных процессов, разработка специфических требований для СУИБ.

Ссылки: 4.2.2, перечисления a) - e), h) O‘z DSt ISO/IEC 27001

При разработке СУИБ должны быть учтены следующие вопросы:

a) безопасность организации - охватывает административные аспекты информационной безопасности, включая ответственность организации за обработку рисков. Из этих аспектов должен быть сформирован комплекс тех видов деятельности, в результате которых будут получены политики, цели, процессы и процедуры обеспечения и улучшения информационной безопасности организации относительно ее потребностей и рисков;

b) безопасность ИКТ - охватывает аспекты информационной безопасности, непосредственно связанные с выполнением операций ИКТ по снижению рисков. Эти аспекты должны обеспечить выполнение требований по снижению рисков, установленных организацией, и внедрение соответствующих технических средств управления;

c) физическая безопасность - охватывает аспекты информационной безопасности, непосредственно связанные с защитой физической среды, например, зданий, сооружений и их инфраструктуры, обеспечивающей снижение рисков. Эти аспекты должны обеспечить выполнение требований по снижению рисков, установленных организацией, и внедрение соответствующих технических средств управления;

d) специфика СУИБ - охватывает аспекты, связанные с различными специфическими требованиями к СУИБ в соответствии с O‘z DSt ISO/IEC 27001, за исключением трех вышеперечисленных областей. Основное внимание уделяется определенным видам деятельности, которые должны выполняться при внедрении СУИБ для обеспечения ее работоспособности, к которым относятся:

1) мониторинг;
2) измерения;
3) внутренний аудит СУИБ;
4) тренинги и повышение осведомленности;
5) управление инцидентами;
6) анализ со стороны руководства;

7) улучшение СУИБ, включая корректирующие и предупреждающие действия.

К разработке проекта СУИБ и запланированному в связи с этим внедрению средств управления необходимо привлекать персонал, имеющий соответствующие навыки и опыт, тех подразделений организации, которые либо находятся в пределах области действия СУИБ, либо на которые возложена ответственность за управление СУИБ. Специфические аспекты СУИБ необходимо обсуждать с руководством.

Для разработки среды безопасности ИКТ, среды физической безопасности и среды безопасности организации крайне необходимой является разработка выбранных средств управления, используемых для обработки рисков. Безопасность ИКТ касается не только информационных систем и сетей, но также и эксплуатационных требований. Физическая безопасность касается всех аспектов управления доступом, неотказуемости, физической защиты информационных активов, хранения информации, а также она является средством защиты для средств управления безопасностью.

Средства управления, выбранные в соответствии с 8.3, должны быть внедрены согласно специфически структурированному и детализированному плану внедрения, являющемуся частью плана проекта СУИБ. В этой конкретной части плана проекта СУИБ должно быть рассмотрено, каким образом для достижения целей управления будет производиться обработка каждого риска. Эта особая часть плана проекта СУИБ является весьма важной, способствующей надлежащему и эффективному внедрению выбранных средств управления. За написание этой особой части плана внедрения отвечает группа управления информационной безопасностью, которая впоследствии разработает окончательный план проекта СУИБ.

9.2 Обеспечение информационной безопасности организации

9.2.1 Разработка окончательной структуры обеспечения информационной безопасности организации

Деятельность

Включение обработки рисков в функции, роли и ответственность в области информационной безопасности организации.

Входные данные

a) выходные данные деятельности 5.3.2 «Определение ролей и ответственности для предполагаемой области действия СУИБ» - таблица ролей и ответственности;

b) выходные данные деятельности 6.5 «Определение области действия и границ СУИБ» - область действия и границы СУИБ;

c) выходные данные деятельности 6.6 «Разработка политики СУИБ и получение разрешения руководства» - политика СУИБ;

d) выходные данные деятельности 7.2 «Определение требований информационной безопасности для процесса СУИБ»;

e) выходные данные деятельности 7.3 «Идентификация активов в пределах области действия СУИБ»;

f) выходные данные деятельности 7.4 «Оценка информационной безопасности»;

g) выходные данные деятельности 8.2 «Определение рисков» - результаты определения рисков;

h) выходные данные деятельности 8.3 «Выбор целей и средств управления»;

i) O‘z DSt ISO/IEC 27002.

Рекомендации

Организационную структуру и процессы эксплуатации для внутренней СУИБ необходимо разрабатывать, при наличии возможности, с учетом изначально существующих областей и, в случае необходимости, интеграции с ними. Также в процессе разработки СУИБ необходимо предусмотреть интеграцию СУИБ с основными изначально существующими структурами управления (например, с внутренним аудитом).

В проектируемой структуре СУИБ организации должна быть отражена деятельность по внедрению и эксплуатации СУИБ, а также должна быть рассмотрена возможность использования в процессе эксплуатации СУИБ соответствующих методов, например, мониторинга и ведения записей.

Соответственно, при разработке структуры эксплуатации СУИБ на основе запланированного внедрения СУИБ должно быть учтено следующее:

a) необходима ли при эксплуатации СУИБ каждая роль, определенная при внедрении СУИБ?

b) отличаются ли определенные роли от ролей, назначенных при внедрении СУИБ?

c) какие роли должны быть добавлены при внедрении СУИБ?

Например, при эксплуатации СУИБ могут быть добавлены следующие роли:

a) лицо, ответственное за обеспечение информационной безопасности в каждом подразделении;

b) лицо, ответственное за измерение СУИБ в каждом подразделении.

Рекомендации, изложенные в приложении B «Распределение ролей и ответственности в области информационной безопасности», помогут принять решение о структуре и ролях при эксплуатации СУИБ путем пересмотра структуры и ролей при внедрении СУИБ.

Выходные данные

Результатом этой деятельности является документ, обобщивший структуру организации, роли и ответственность.

Дополнительная информация

Дополнительная информация приведена в следующих приложениях:

- приложение B «Распределение ролей и ответственности в области информационной безопасности»;
- приложение C «Внутренний аудит».

9.2.2 Разработка структуры документации СУИБ

Деятельность

Управление записями и документами СУИБ должно производиться в соответствии с установленными требованиями и структурой, которая позволяет выполнять требования по текущему управлению записями и документами СУИБ.

Входные данные

a) выходные данные деятельности 6.5 «Определение области действия и границ СУИБ» - область действия и границы СУИБ;

b) выходные данные деятельности 6.6 «Разработка политики СУИБ и получение разрешения руководства» - политика СУИБ;

c) выходные данные деятельности 8.4 «Получение разрешения руководства на внедрение и эксплуатацию СУИБ»;

d) выходные данные деятельности 9.2.1 «Разработка окончательной структуры обеспечения информационной безопасности организации»;

e) O‘z DSt ISO/IEC 27002.

Рекомендации

Для системы ведения записей СУИБ необходимо разработать:

a) основные правила документирования СУИБ, структуру документированных процедур СУИБ, задействованные роли, форматы данных и способы предоставления отчетности руководству;

b) требования к документации;

c) требования к ведению записей.

Документация СУИБ должна включать записи принимаемых руководством решений; обеспечивать прослеживание деятельности по выполнению решений руководства и требований политик, а также воспроизводимость записанных результатов.

В документах СУИБ должны быть представлены доказательства того, что средства управления были выбраны с учетом результатов определения и обработки рисков, и что наряду с политикой и целями СУИБ были внедрены и эти процессы.

Документация необходима для обеспечения воспроизводимости результатов и процедур. При установлении и документировании процедур для выбранных средств управления должно указываться лицо, ответственное за актуальную часть документации.

Состав документации СУИБ определен в 4.3.1 O‘z DSt ISO/IEC 27001.

Необходимо осуществлять управление документами СУИБ и обеспечивать их доступность для персонала при необходимости. Эта деятельность включает:

a) установление административной процедуры управления документами СУИБ;

b) надлежащее утверждение документов перед их изданием;

c) обеспечение идентификации внесенных изменений и текущего статуса документов;

d) защиту и управление документами таким же образом, как и информационными активами организации.

Важно, чтобы соответствующие версии используемых документов были доступны в местах их применения, чтобы документы были удобочитаемы и легко идентифицируемы и чтобы их передача, хранение и, в конечном итоге, уничтожение проводилось в соответствии с процедурами, применимыми к степени их конфиденциальности.

Кроме того, необходимо обеспечить идентификацию документов внешнего происхождения, контроль за распространением документов, предотвращение непреднамеренного использования устаревших документов и, в случае дальнейшего хранения с какой-либо целью, осуществлять их соответствующее отслеживание.

Для предоставления свидетельств соответствия требованиям O‘z DSt ISO/IEC 27001 и демонстрации эффективности операций СУИБ в организации должны вестись, поддерживаться в рабочем состоянии и контролироваться записи.

Также необходимо хранить записи хода выполнения всех фаз модели «планирование - осуществление - проверка – действие», а также записи об инцидентах и событиях информационной безопасности, записи об обучении, тренингах, навыках, опыте и квалификации персонала, записи о результатах внутреннего аудита СУИБ, записи о корректирующих и профилактических действиях и записи организации.

При управлении записями должны выполняться следующие задачи:

a) документирование средств управления, необходимых для идентификации, хранения, защиты, поиска и удаления данных, и документирование сроков хранения записей;

b) определение того, что и насколько подробно должно записываться в процессах оперативного управления;

c) если какой-либо срок хранения установлен правовыми нормами или законодательством, то срок хранения записей должен соответствовать требованиям этого законодательства.

Выходные данные

Результатами этой деятельности являются:

a) документ, содержащий требования по управлению записями и документами СУИБ;

b) репозитории и шаблоны соответствующих записей СУИБ.

Дополнительная информация

Дополнительная информация отсутствует.

9.2.3 Разработка политики информационной безопасности

Деятельность

Документирование стратегических целей руководства и администрации в области информационной безопасности относительно функционирования СУИБ.

Входные данные

a) выходные данные деятельности 5.2 «Определение приоритетов организации при разработке СУИБ» - обобщенные цели и перечень требований;

b) выходные данные деятельности 5.4 «Разработка экономического обоснования, план проекта и получение разрешения руководства» - разрешение руководства на инициацию проекта СУИБ;

c) выходные данные деятельности 6.5 «Определение области действия и границ СУИБ» - область действия и границы СУИБ;

d) выходные данные деятельности 6.6 «Разработка политики СУИБ и получение разрешения руководства» - политика СУИБ;

e) выходные данные деятельности 7.2 «Определение требований информационной безопасности для процесса СУИБ»;

f) выходные данные деятельности 7.3 «Идентификация активов в пределах области действия СУИБ»;

g) выходные данные деятельности 7.4 «Оценка информационной безопасности»;

h) выходные данные деятельности 8.2 «Определение рисков» - результаты определения рисков, выходные данные деятельности 8.3 «Выбор целей и средств управления»;

i) выходные данные деятельности 9.2.1 «Разработка окончательной структуры обеспечения информационной безопасности организации»;

j) выходные данные деятельности 9.2.2 «Разработка структуры документации СУИБ»;

k) 5.1.1 O‘z DSt ISO/IEC 27002.

Рекомендации

В политике информационной безопасности документируются стратегические цели организации относительно информационной безопасности всей организации.

Политика разрабатывается на основе информации и знаний. Важность тех факторов, которые во время ранее проведенного анализа были определены руководством, должна быть очевидной и для стимулирования и мотивации персонала организации в области информационной безопасности в политике на них должно быть акцентировано внимание. Также важно отметить, каковы будут последствия нарушений политики. Следует также отметить влияние нормативно-правовых актов, которые затрагивают рассматриваемую организацию.

Примеры политики информационной безопасности можно найти в справочной литературе, сети Интернет, ассоциациях по интересам и отраслевых ассоциациях. Формулировки и фразы могут быть позаимствованы из годовых отчетов, документов другой политики или других утвержденных руководством документов.

Относительно фактического объема политики могут существовать различные интерпретации и требования. Политика должна быть достаточно краткой, доступной и понятной для персонала организации. Кроме того, в политике должны быть достаточно полно рассмотрены цели, необходимые для выполнения ряда инструкций и целей организации.

Объем и структура политики информационной безопасности должны дополняться документами, которые будут использованы на следующем этапе - в процессе внедрения СУИБ в соответствии с приложением D.

Для больших организаций, имеющих сложную структуру (например, организаций, осуществляющих деятельность в различных сферах), может быть будет необходима разработка общей политики и множества политик более низкого уровня для конкретных видов деятельности.

Рекомендации по документированию политики информационной безопасности приведены в 5.1.1 O‘z DSt ISO/IEC 27002.

Предложенная политика (с номером версии и датой) должна быть повторно проверена и согласована с соответствующим должностным лицом организации. После того, как политика информационной безопасности будет согласована отделом обеспечения информационной безопасности или аналогичным подразделением, соответствующее должностное лицо ее утверждает. Затем политика информационной безопасности доводится до сведения всего персонала организации в доступной и понятной форме.

Выходные данные

Результатом этой деятельности является документированная политика информационной безопасности.

Дополнительная информация

Дополнительная информация приведена в следующих приложениях:

- приложение B «Распределение ролей и ответственности в области информационной безопасности»;
- приложение D «Структура политик».

9.2.4 Разработка стандартов и процедур информационной безопасности

Деятельность

Разработка стандартов и процедур информационной безопасности для всей организации или отдельных ее подразделений.

Входные данные

a) выходные данные деятельности 6.5 «Определение области действия и границ СУИБ» - область действия и границы СУИБ;

b) выходные данные деятельности 6.6 «Разработка политики СУИБ и получение разрешения руководства» - политика СУИБ;

c) выходные данные деятельности 8.2 «Определение рисков»;

d) выходные данные деятельности 8.3 «Выбор целей и средств управления»;

e) выходные данные деятельности 8.4 «Получение разрешения руководства на внедрение и эксплуатацию СУИБ» - заявление о применимости, в том числе цели и выбранные средства управления;

f) выходные данные деятельности 9.2.1 «Разработка окончательной структуры обеспечения информационной безопасности организации»;

g) выходные данные деятельности 9.2.2 «Разработка структуры документации СУИБ»;

h) выходные данные деятельности 9.2.3 «Разработка политики информационной безопасности»;

i) O‘z DSt ISO/IEC 27002.

Рекомендации

Для обоснования работ в области информационной безопасности для тех должностных лиц организации, кому это положено знать, должны быть доступны стандарты информационной безопасности, а также комплект применимых к организации требований нормативно-правовых актов.

В процессе разработки стандартов и процедур должны участвовать представители различных подразделений организации, попадающих в область действия СУИБ. Участники этого процесса должны иметь соответствующие полномочия и быть представителями организации. К примеру, могут быть включены следующие роли:

a) администраторы информационной безопасности;

b) представители подразделения, обеспечивающего физическую безопасность;

c) владельцы информационных систем;

d) владельцы процессов стратегических и эксплуатационных подразделений.

Это позволит создать рабочую группу с минимумом членов с возможностью (при необходимости) привлечения специалистов в эту группу на временной основе. Каждый представитель должен активно поддерживать связь со своим подразделением организации для обеспечения непрерывной оперативной поддержки. Это впоследствии облегчит последующее улучшение процедур и программ на оперативном уровне.

Впоследствии стандарты и процедуры безопасности должны использоваться в качестве основы для проектирования подробных технических или оперативных процедур.

Эффективным методом разработки стандартов и процедур информационной безопасности является рассмотрение каждого пункта рекомендаций, содержащихся в O‘z DSt ISO/IEC 27001 и O‘z DSt ISO/IEC 27002, который считается применимым (по результатам определения рисков), и точное описание применения этого пункта.

Все существующие стандарты и процедуры информационной безопасности периодически следует подвергать экспертизе. Например, на предмет необходимости внесения в них изменений и пересмотра, или их полной замены.

Каждому сотруднику, находящемуся в области действия СУИБ, должны быть предоставлены самые последние версии соответствующих документов. Стандарты и процедуры информационной безопасности должны применяться ко всей организации или содержать пояснения, на какие роли, системы и подразделения они распространяются. Первая версия должна быть выпущена своевременно.

Процессы экспертизы и пересмотра должны быть определены на раннем этапе. Впоследствии необходимо будет предусмотреть, каким образом будет распространяться информация об изменении политики.

Выходные данные

Результатами этой деятельности являются:

a) структурированный и детализированный план внедрения средств управления безопасностью организации, являющийся частью окончательного плана проекта СУИБ, включая документированную структуру комплекта стандартов в области информационной безопасности;

b) стандарты в области информационной безопасности, в том числе исходные данные организации;

c) процедуры информационной безопасности, необходимые для выполнения требований стандартов в области информационной безопасности.

Дополнительная информация

Дополнительная информация приведена в приложении D «Структура политик».

9.3 Обеспечение информационной и физической безопасности ИКТ

Деятельность

Разработка средств управления для ИКТ и физической безопасности окружающей их среды.

Входные данные

a) выходные данные деятельности 6.5 «Определение области действия и границ СУИБ» - область действия и границы СУИБ;

b) выходные данные деятельности 6.6 «Разработка политики СУИБ и получение разрешения руководства» - политика СУИБ;

c) выходные данные деятельности 7.2 «Определение требований информационной безопасности для процесса СУИБ»;

d) выходные данные деятельности 7.3 «Идентификация активов в пределах области действия СУИБ»;

e) выходные данные деятельности 7.4 «Оценка информационной безопасности»;

f) выходные данные деятельности 8.3 «Выбор целей и средств управления»;

g) выходные данные деятельности 8.4 «Получение разрешения руководства на внедрение и эксплуатацию СУИБ» - заявление о применимости, в том числе цели и выбранные средства управления;

h) O‘z DSt ISO/IEC 27002.

Рекомендации

В этой деятельности для каждого средства управления, которое должно быть частью плана проекта СУИБ, должна быть задокументирована следующая информация:

a) лицо, ответственное за внедрение средства управления;

b) приоритет внедрения средства управления;

c) задачи или виды деятельности по внедрению средств управления;

d) сроки внедрения средств управления;

e) лицо, которому должен быть представлен отчет после завершения внедрения средств управления;

f) ресурсы, необходимые для внедрения средств управления (количество персонала, потребность в ресурсах, требования по размещению, расходы).

Изначально безопасность ИКТ и физическая безопасность должны быть разработаны концептуально. При этом необходимо учесть следующее.

Ответственность за процесс инициации внедрения обычно включает:

a) спецификацию целей управления с описанием будущего планируемого состояния;

b) распределение ресурсов (объем работ, финансовые ресурсы);

c) сроки внедрения средства управления;

d) варианты интеграции безопасности ИКТ, физической безопасности и безопасности организации.

По завершению разработки концепции необходимо разработать реальный проект, например, разработать систему для организации с учетом современных тенденций и передового опыта. При этом следует учесть следующее.

Ответственность за процесс фактического внедрения включает:

a) разработку для каждого из выбранных средств управления для ИКТ, физической и организационных сфер на операционном уровне рабочего места;

b) установку каждого средства управления в соответствии с согласованным проектом;

c) предоставление методики и информации о средствах управления безопасностью для курсов повышения квалификации персонала и тренингов;

d) предоставление вспомогательных средств и внедрение средств управления на рабочем месте.

Проведение четкой грани между начальной и заключительной частями процесса внедрения не всегда может быть уместно или необходимо, это зависит от типа средств управления (ИКТ, физические или организационные).

При внедрении средств управления часто необходимо взаимодействовать нескольким различным ролям в пределах организации. Например, системные администраторы должны будут приобрести, установить и эксплуатировать технические средства. Другие роли могут лучше подходить для разработки и документирования порядка применения систем.

Информационная безопасность должна быть интегрирована в процедуры и процессы всей организации. Если для некоторых подразделений организации или третьей стороны внедрение средств управления окажется затруднительным, то соответствующие стороны должны сообщить об этом немедленно, чтобы можно было совместно решить эту проблему. Решение проблемы такого типа заключается в изменении процедур и процессов, перераспределении ролей и ответственности, а также адаптации технических процедур.

Результатами внедрения средств управления СУИБ должны стать:

a) план внедрения, в котором детально описано внедрение средств управления, например, график, состав группы внедрения и т.д.;

b) записи и документирование результатов внедрения.

Выходные данные

Результатом этой деятельности является структурированный и детализированный план внедрения средств управления для ИКТ и физической безопасности, являющийся частью плана проекта СУИБ и включающий для каждого средства управления:

a) подробное описание;

b) перечень лиц, ответственных за разработку и внедрение;

c) ожидаемые сроки;

d) включенные задачи;

e) требуемые ресурсы;

f) владение (субординация).

Дополнительная информация

Дополнительная информация отсутствует.

9.4 Обеспечение информационной безопасности конкретной СУИБ

9.4.1 План анализа со стороны руководства

Деятельность

Разработка плана анализа функционирования СУИБ с участием руководства, результаты которого будут способствовать ее непрерывному улучшению.

Входные данные

a) выходные данные деятельности 6.5 «Определение области действия и границ СУИБ» - область применения и границы СУИБ;

b) выходные данные деятельности 6.6 «Разработка политики СУИБ и получение разрешения руководства» - политика СУИБ;

c) выходные данные деятельности 8.4 «Получение разрешения руководства на внедрение и эксплуатацию СУИБ» - заявление о применимости, в том числе цели и выбранные средства управления;

d) выходные данные деятельности 9.2.3 «Разработка политики информационной безопасности»;

e) O‘z DSt ISO/IEC 27004.

Рекомендации

Анализ функционирования СУИБ со стороны руководства следует проводить, начиная с самых ранних этапов разработки ее спецификации и экономического обоснования, а впоследствии – периодически, через установленные промежутки времени. Непосредственное участие руководства позволяет подтвердить соответствие СУИБ потребностям бизнеса и поддерживать обязательства бизнеса относительно СУИБ.

Планирование анализа со стороны руководства включает установление сроков и способов его проведения. Подробная информация

об исходных данных, необходимых для проведения анализа со стороны руководства, приведена в 7.2 O‘z DSt ISO/IEC 27001.

При планировании анализа должны быть определены все роли, которые должны принять в нем участие. Выбранные роли должны быть утверждены руководством и должны быть как можно раньше об этом проинформированы. Целесообразно предоставить руководству необходимые данные относительно необходимости и целей процесса анализа. (Более подробная информации приведена в приложении B «Распределение ролей и ответственности в области информационной безопасности».)

Анализ со стороны руководства должен быть основан на результатах измерений СУИБ и другой информации, собранной за время функционирования СУИБ. Эта информация используется в деятельности руководства СУИБ для определения уровня зрелости и эффективности СУИБ. Необходимые входные и выходные данные для анализа СУИБ приведены в O‘z DSt ISO/IEC 27001, а дополнительная информация относительно измерений СУИБ приведена в приложении E и O‘z DSt ISO/IEC 27004.

Также следует отметить, что этот анализ должен включать анализ методологии и результатов определения рисков. Анализ должен проводиться в запланированные сроки, с учетом любых изменений в среде, например, изменений структуры организации и технологии.

Для того, чтобы после внедрения СУИБ имелась возможность регулярной ее оценки, составляется план проведения внутреннего аудита. Важными исходными данными для анализа со стороны руководства являются результаты внутреннего аудита СУИБ. Следовательно, до проведения анализа со стороны руководства должно быть запланировано проведение внутреннего аудита СУИБ. Внутренний аудит СУИБ должен включать проверку эффективности целей управления, процессов или процедур СУИБ, а также внедренных и эксплуатируемых средств управления и их соответствия:

a) требованиям O‘z DSt ISO/IEC 27001;

b) требованиям соответствующих нормативно-правовых актов;

c) определенным требованиям информационной безопасности.

(Дополнительная информация относительно планирования аудита приведена в приложении C.)

Непременным условием для проведения анализа со стороны руководства является наличие собранной информации о внедрении и эксплуатации СУИБ. В информацию, предоставляемую группе, которая проводит анализ со стороны руководства, может быть включено следующее:

a) отчет об инцидентах за последний период эксплуатации;

b) подтверждение эффективности управления и определенные несоответствия;

c) результаты предыдущих аудитов и анализов (более подробные, если были выявлены несоответствия требованиям политики);

d) рекомендации по улучшению СУИБ.

В плане мониторинга должно быть предусмотрено документирование результатов мониторинга, которые должны быть записаны и доложены руководству (дополнительная информация относительно мониторинга приведена в приложении Е).

Выходные данные

Результатом этой деятельности является документ, в котором содержится план, необходимый для организации анализа со стороны руководства, и в котором рассматриваются:

a) исходные данные, необходимые для проведения анализа со стороны руководства;

b) процедуры, выполняемые при проведении анализа со стороны руководства, охватывающие аспекты аудита, мониторинга и измерений.

Дополнительная информация

Дополнительная информация приведена в следующих приложениях:

- приложение В «Распределение ролей и ответственности в области информационной безопасности»;
- приложение С «Внутренний аудит»;
- приложение Е «Мониторинг и измерения».

9.4.2 Разработка программ повышения осведомленности, обучения и тренингов в области информационной безопасности

Деятельность

Разработка программы повышения осведомленности, обучения и тренингов персонала организации в области информационной безопасности.

Входные данные

a) выходные данные деятельности 6.5 «Определение области действия и границ СУИБ» - область действия и границы СУИБ;

b) выходные данные деятельности 6.6 «Разработка политики СУИБ и получение разрешения руководства» - политика СУИБ;

c) выходные данные деятельности 7.2 «Определение требований информационной безопасности для процесса СУИБ» - в части требований по обучению и тренингов в области информационной безопасности персонала организации;

d) выходные данные деятельности 8.4 «Получение разрешения руководства на внедрение и эксплуатацию СУИБ» - заявление о применимости, в том числе цели и выбранные средства управления;

e) выходные данные деятельности 8.3 «Выбор целей и средств управления» - план обработки рисков;

f) выходные данные деятельности 9.2.3 «Разработка политики информационной безопасности»;

g) выходные данные деятельности 9.2.4 «Разработка стандартов и процедур информационной безопасности»;

h) анализ общей программы обучения и тренингов персонала организации.

Рекомендации

За организацию обучения и тренингов отвечает руководство, это способствует тому, чтобы весь персонал с четко определенными ролями имел знания и навыки, необходимые для выполнения соответствующих операций. Желательно, чтобы содержание проводимых обучения и тренингов помогло всему персоналу осознать и понять значение и важность деятельности в области информационной безопасности, в которую они вовлечены, и то, каким образом они могут способствовать достижению целей СУИБ.

На данном этапе очень важно обеспечить, чтобы каждый служащий в пределах области действия СУИБ прошел необходимые тренинги и/или обучение в области информационной безопасности. В больших организациях, как правило, недостаточно иметь материал для тренингов одного содержания, так как он будет содержать слишком много данных, которые важны только для конкретных видов работы, и, следовательно, будет большим, сложным и трудным для восприятия. В таких случаях обычно следует иметь разные наборы материалов для тренингов, предназначенные для всех основных ролей, например, для офисных служащих, ИТ-персонала или для операторов, которые адаптированы к конкретным потребностям этих сотрудников.

В программе повышения осведомленности, обучения и тренингов в области информационной безопасности должно быть предусмотрено ведение записей о проводимых тренингах и обучении. Эти записи должны регулярно просматриваться, это будет гарантией того, что весь персонал прошел необходимые тренинги. Необходимо назначить должностное лицо, ответственное за этот процесс.

Материалы тренингов по информационной безопасности должны разрабатываться во взаимосвязи с материалами других тренингов, используемых организацией, особенно с материалами курсов подготовки пользователей информационных систем. Желательно, чтобы тренинги по важным аспектам информационной безопасности были включены во все курсы для пользователей ИТ.

В зависимости от целевой аудитории в материалах тренингов по информационной безопасности, как минимум, должны быть рассмотрены следующие темы:

a) риски и угрозы информационной безопасности;

b) основные термины в области информационной безопасности;

c) четкое определение инцидента безопасности: рекомендации по его обнаружению, устранению его последствий и отчетности;

d) политика, стандарты и процедуры в области информационной безопасности организации;

e) ответственность и способы предоставления отчетности в области информационной безопасности организации;

f) рекомендации по улучшению информационной безопасности;

g) рекомендации по инцидентам и отчетности информационной безопасности;

h) источники получения дополнительной информации.

Для проведения тренингов по информационной безопасности должна быть определена группа, способная выполнять следующие задачи:

a) создание и управление записями тренингов;

b) создание и управление материалами тренингов;

c) проведение тренингов.

Эти задачи могут быть распределены между персоналом, проводящим тренинги. Но этот персонал может потребовать проведения фундаментального тренинга относительно концепций информационной безопасности, чтобы обеспечить их эффективное и точное представление.

Программа повышения осведомленности, обучения и тренингов в области информационной безопасности должна включать процедуру, гарантирующую, что материалы тренингов регулярно пересматриваются и корректируются. Следует назначить должностное лицо, ответственное за пересмотр и корректировку материалов тренингов.

Выходные данные

Результатами этой деятельности являются:

a) материалы по повышению осведомленности, обучению и тренингам в области информационной безопасности;

b) разработка программ повышения осведомленности, обучения и тренингов в области информационной безопасности;

c) планы повышения осведомленности, обучения и тренингов в области информационной безопасности;

d) текущие записи, показывающие результаты повышения осведомленности, обучения и тренингов персонала в области информационной безопасности.

Дополнительная информация

Дополнительная информация отсутствует.

9.5 Разработка окончательного плана проекта СУИБ

Деятельность

Разработка окончательного плана проекта СУИБ, включающего те виды деятельности, которые необходимы для внедрения выбранных средств управления.

Входные данные

a) выходные данные деятельности 6.5 «Определение области действия и границ СУИБ» - область действия и границы СУИБ;

b) выходные данные деятельности 6.6 «Разработка политики СУИБ и получение разрешения руководства» - политика СУИБ;

c) выходные данные деятельности 9.2 «Обеспечение информационной безопасности организации»;

d) выходные данные деятельности 9.3 «Обеспечение информационой безопасности ИКТ и физической безопасности»;

e) выходные данные деятельности 9.4 «Обеспечение информационной безопасности конкретной СУИБ»;

f) O‘z DSt ISO/IEC 27002.

Рекомендации

Виды деятельности, необходимые для внедрения выбранных средств управления и выполнения других видов деятельности, связанных с СУИБ, должны быть оформлены в виде детального плана внедрения, как части окончательного проекта СУИБ. Детальный план внедрения также может быть дополнен описаниями инструментальных средств и методов, предлагаемых к внедрению. В проекте СУИБ организации подразумевается появление множества различных ролей, поэтому важно, чтобы соответствующие виды деятельности были четко распределены между ответственными сторонами и чтобы на начальных фазах проекта с планом внедрения был ознакомлен весь соответствующий персонал организации.

И, наконец, очень важный момент: лицо, ответственное за проект, должно обеспечить для внедрения проекта выделение достаточных ресурсов.

Выходные данные

Результатом этой деятельности является окончательный план проекта внедрения СУИБ.

Дополнительная информация

Дополнительная информация отсутствует.

Приложение А
(справочное)

Контрольная таблица

Цель:

- предоставить контрольную таблицу, содержащую описание деятельности, необходимой для разработки и внедрения СУИБ;
- организовать мониторинг хода выполнения внедрения СУИБ;
- установить взаимосвязь деятельности по внедрению СУИБ с соответствующими требованиями O‘z DSt ISO/IEC 27001.

Контрольная таблица приведена в таблице А.1

Таблица А.1

Фаза внедрения O‘z DSt ISO/IEC 27003	Номер этапа	Деятельность, ссылка на O‘z DSt ISO/IEC 27003	Предварительное требование	Выходные документы	Ссылка на O‘z DSt ISO/IEC 27001
1	2	3	4	5	6
5 Получение разрешения руководства на внедрение СУИБ	1	Сбор бизнес-целей организации	нет	Перечень бизнес-целей организации	отсутствует
	2	Понимание преимуществ существующих систем управления	нет	Описания существующих систем управления	отсутствует
	3	5.2 Определение приоритетов организации при разработке СУИБ	1, 2	Краткое изложение целей, приоритетов в области информационной безопасности и требований организации к СУИБ	отсутствует

Продолжение таблицы А.1

1	2	3	4	5	6
	4	Сбор соответствующих нормативно-правовых актов, государственных и отраслевых стандартов, применимых к организации	нет	Перечень нормативно-правовых актов, государственных и отраслевых стандартов, применимых к организации	отсутствует
	5	5.3 Определение предполагаемой области действия СУИБ	3, 4	Описание предполагаемой области действия СУИБ (5.3.1)	отсутствует
				Определение ролей и ответственности (5.3.2)	отсутствует
	6	5.4 Разработка экономического обоснования, плана проекта и получение разрешения руководства	5	Экономическое обоснование и предложенный план проекта	отсутствует
	7	Получение разрешения руководства и обязательств по инициации проекта внедрения СУИБ	6	Разрешение руководства на инициацию проекта внедрения СУИБ	отсутствует
6 Определение области действия, границ и политики СУИБ	8	6.2 Определение области действия и границ организации	7	Описание границ организации Функции и структура организации Информация, обмен которой происходит через границы Бизнес-процессы и ответственность за информационные активы в пределах области действия СУИБ и за ее пределами	4.2.1, перечисление а) (частично)
	9	6.3 Определение области действия и границ ИКТ	7	Описание границ ИКТ Описание информационных систем и сетей телекоммуникаций в пределах области действия СУИБ и за ее пределами	4.2.1, перечисление а) (частично)

Продолжение таблицы А.1

1	2	3	4	5	6
	10	6.4 Определение физических области действия и границ	7	Описание физических границ СУИБ Описание организации и ее географических характеристик относительно области действия СУИБ	4.2.1, перечисление a) (частично)
	11	6.5 Определение области действия и границ СУИБ	8, 9, 10	Документ, содержащий описание области действия и границ СУИБ	4.2.1, перечисление a)
	12	6.6 Разработка политики СУИБ и получение разрешения руководства	11	Политика СУИБ, утвержденная руководством	4.2.1, перечисление b)
7 Анализ требований информационной безопасности	13	7.2 Определение требований информационной безопасности для процесса СУИБ	12	Перечень основных процессов, функций, местоположений, информационных систем, сетей телекоммуникаций	отсутствует
				Требования организации относительно конфиденциальности, доступности и целостности информации	отсутствует
				Требования организации в области информационной безопасности, полученные из требований нормативно-правовых актов, требований договоров и бизнеса	4.2.1, перечисление c) 1) (частично)
				Перечень общеизвестных уязвимостей	4.2.1, перечисление d) 3)

Продолжение таблицы А.1

1	2	3	4	5	6
	14	7.3 Идентификация активов в пределах области действия СУИБ	13	Описание основных процессов организации Идентификация информационных активов основных процессов организации в пределах области действия СУИБ Классификация критических процессов/активов	отсутствует 4.2.1, перечисление d) 1) отсутствует
	15	7.4 Оценка информационной безопасности	14	Документ организации, содержащий описание реального состояния и оценку ее информационной безопасности, в т.ч. существующих средств управления информационной безопасностью Документ организации, содержащий описание обнаруженных и оцененных уязвимостей	4.2.1, перечисление e) 2) (частично)
8 Определение рисков и выбор вариантов обработки рисков	16	8.2 Определение рисков	15	Область действия для определения рисков Утвержденная методология определения рисков, соответствующая контексту стратегического управления рисками организации Критерии принятия рисков	4.2.1, перечисление c) 1)
	17	8.3 Выбор целей и средств управления	16	Документированное определение рисков высокого уровня	4.2.1, перечисление e) 3) (частично)

Продолжение таблицы А.1

1	2	3	4	5	6
				Определение необходимости в дополнительном глубоком определении рисков	отсутствует
				Документированное глубокое определение рисков	4.2.1 e) 3) (частично)
				Обобщенные результаты определения рисков	отсутствует
	18	8.4 Получение разрешения руководства на внедрение и функционирование СУИБ	17	Риски и определенные варианты их обработки	4.2.1, перечисление f)
				Выбранные цели и средства управления для обработки рисков	4.2.1, перечисление g)
	19	Принятие руководством остаточных рисков	18	Документированное принятие руководством предлагаемых остаточных рисков (должно быть выходыми даными 8.4)	4.2.1, перечисление h)
	20	Разрешение руководства на внедрение и функционирование СУИБ	19	Документированное разрешение руководства на внедрение и функционирование СУИБ (должно быть выходными даными 8.4)	4.2.1, перечисление i)
	21	Составление заявления о применимости	18	Заявление о применимости	4.2.1, перечисление j)
9 Разработка СУИБ	22	9.2 Обеспечение информационной безопасности организации	20	Документ, описывающий структуру организации, обеспечение ее информационной безопасности, а также роли и ответственность	5.1, перечисление c)

Продолжение таблицы А.1

1	2	3	4	5	6
				Структура документации СУИБ Шаблоны записей СУИБ и инструкции по их использованию и хранению Документированная политика информационной безопасности Исходные данные для разработки политик информационной безопасности и процедур (с прилагаемыми планами разработки конкретных политик, процедур и т.п.)	4.3 O‘z DSt ISO/IEC 27002; 5.1.1
	23	9.3 Обеспечение информационной и физической безопасности ИКТ	20, 21	Планы проекта внедрения в части процессов внедрения выбранных средств управления информационной и физической безопасностью ИКТ	4.2.2, перечисление c) (частично)
	24	9.4 Обеспечение информационной безопасности конкретной СУИБ	22, 23	Документированные процедуры, описывающие процессы отчетности и анализа со стороны руководства	7.1
	25			Описания процедур аудита, мониторинга и измерений	4.2.3, перечисление a) (частично); 4.2.3, перечисление b) (частично); 6

Окончание таблицы А.1

1	2	3	4	5	6
	26			Программа тренингов и повышения осведомленности	5.2.2
	27	9.5 Разработка окончательного плана проекта СУИБ	25	План проекта внедрения в части процессов внедрения, утвержденный руководством	отсутствует
	28	Окончательный план проекта СУИБ	28	План проекта внедрения конкретной СУИБ организации, предусматривающий обеспечение информационной безопасности организации, информационной и физической безопасности ИКТ, а также выполнение специфических требований, полученных в результате деятельности в соответствии с O‘z DSt ISO/IEC 27003	отсутствует

Приложение B
(справочное)

Распределение ролей и ответственности в области информационной безопасности

Это приложение содержит дополнительные рекомендации по распределению ролей и ответственности в организации в области информационной безопасности. Ниже приведены роли, необходимые при внедрении СУИБ в организации.

B.1 Роль Комитета по информационной безопасности

Комитет по информационной безопасности должен играть ведущую роль в СУИБ организации. Комитет по информационной безопасности должен отвечать за обработку информационных активов организации и обладать соответствующими основными сведениями в области информационной безопасности, необходимыми для управления, мониторинга и завершения необходимых задач.

Ниже приведены примеры возможных ролей комитета по информационной безопасности:

a) завершение управления рисками, формирование плана работы с документами СУИБ, ответственность за определение содержания этих документов и получение одобрения руководства;

b) планирование приобретения нового оборудования и/или принятие решения о повторном использовании существующего оборудования, которым организация уже располагает;

c) решение любых возникающих проблем;

d) рассмотрение улучшений, которые могут быть получены в результате последующего внедрения и измерения СУИБ;

e) осуществление стратегического руководства СУИБ (как во время реализации проекта, так и во время работы);

f) обеспечение взаимодействия между высшим руководством, группой по внедрению проекта и персоналом, задействованным в области информационной безопасности.

B.2 Роль Группы планирования информационной безопасности

В планировании проекта, выполняемого группой проекта СУИБ, должны принимать участие те сотрудники организации, которые хорошо осведомлены о важных информационных активах в пределах области действия СУИБ и имеют достаточные знания для рассмотрения возможности обработки этой информации. Например, по вопросам обработки информационных активов среди подразделений в пределах области действия СУИБ могут существовать разные мнения, поэтому может возникнуть необходимость в корректировке положительных и

отрицательных воздействий на план. Группе проекта необходимо выступать в роли координатора при устранении противоречий между подразделениями. Для этого членам группы необходимо иметь навыки общения, приобретенные за время работы, и способности координирования, а также высокий уровень знания в области безопасности.

B.3 Специалисты и внешние консультанты

До начала внедрения СУИБ организация должна выбрать сотрудников для выполнения вышеперечисленных обязанностей (при наличии возможности этим сотрудникам должна быть назначена только одна роль). Вместе с тем эти сотрудники должны иметь обширные знания и опыт в области информационной безопасности, а также в таких областях, как «информационные технологии», «управленческие решения» и «понимание организации».

Лица, ответственные за выполнение данных операций в организации, могут знать эти специфические области наилучшим образом. Большинство специалистов, которые являются экспертами в специфических областях этой организации, должны привлекаться к разработке СУИБ, если она будет затрагивать их специфические области. Для достижения целей организации важно также соблюсти баланс между компетентностью и обширными знаниями этих специалистов.

Внешние консультанты могут давать рекомендации, основанные на объективной оценке ими ситуации в организации и их опыте работы в других аналогичных случаях, даже если они обычно не обладают глубокими знаниями относительно специфики организации и подробной информацией об ее работе.

Не обязательно использовать термины, приведенные в вышеуказанных примерах, такие как «комитет по информационной безопасности» и «группа планирования информационной безопасности». Должна быть понятна только функция каждой структуры. Желательно иметь внутренние структуры, которые должны будут координировать информационную безопасность организации, обмениваться информацией и тесно взаимодействовать с каждым техническим подразделением.

B.4 Владельцы информационных активов

Для каждого процесса и специализированной области организации должен быть назначен сотрудник; этот сотрудник будет являться так называемым «владельцем информационного актива» по всем вопросам информационной безопасности относительно обработки данных в рамках этого конкретного процесса. Контактное лицо или владелец процесса отвечает, например, за выдачу задач и обработку информации в рамках процессов организации, для которых они предназначены.

В случае распределения, исключения и удержания рисков должны быть предприняты необходимые действия в соответствии с организационными аспектами безопасности. Если принято решение о передаче рисков, то будет необходимо, например, заключить контракты со страховой компанией, товариществом и совместными предприятиями, тем самым ответственность за риски будет перенесена на них.

На рисунке В.1 показан пример организационной структуры создаваемой СУИБ. На этом примере основаны нижеприведенные основные роли и ответственность в организации.

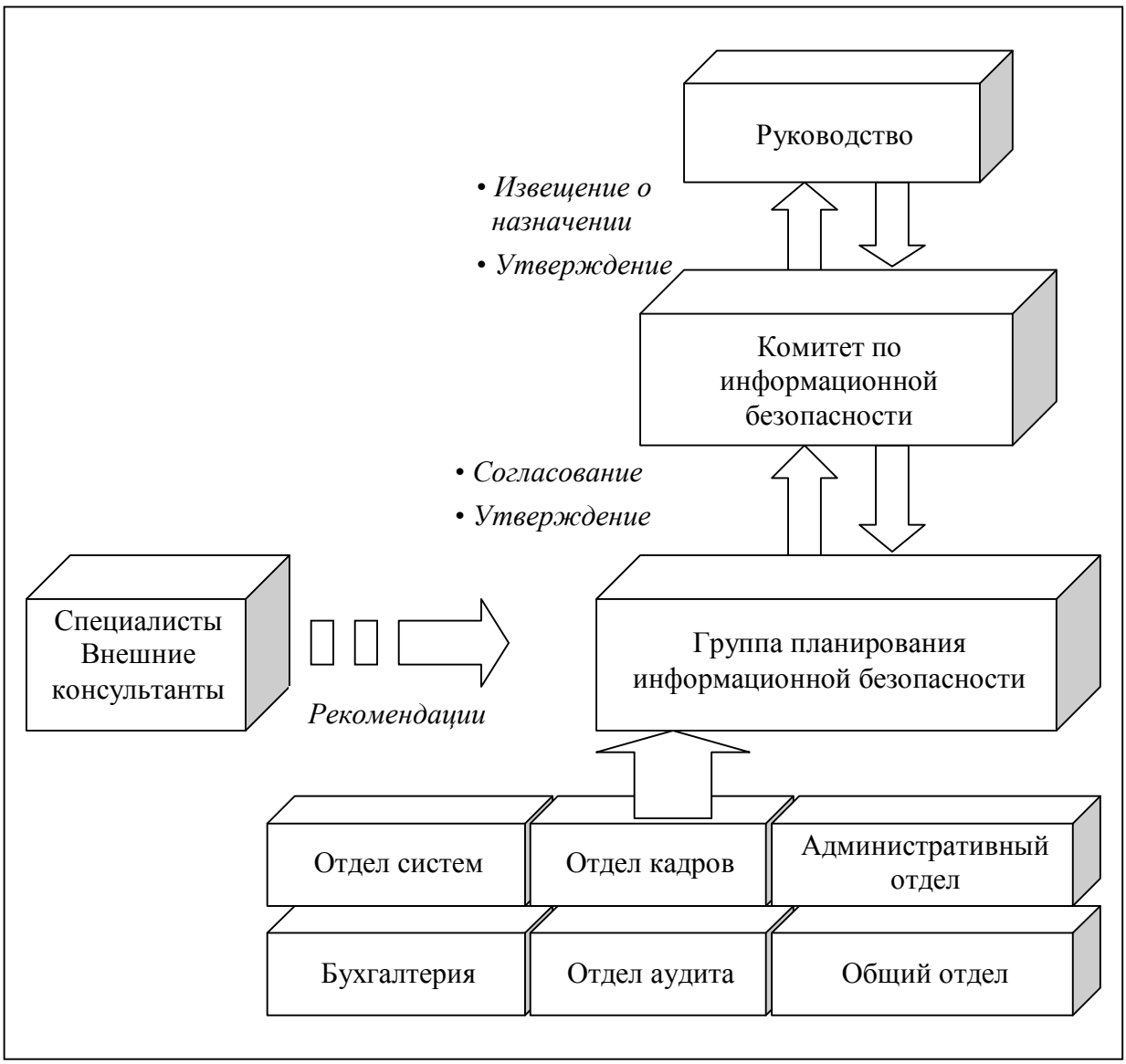


Рисунок В.1 - Пример организационной структуры создаваемой СУИБ

Взаимодействие с организацией

Все вовлеченные стороны должны тщательно ознакомиться с существующими требованиями по защите активов организации.

В проведении анализа организации должны принимать участие сотрудники, отлично знающие как организацию, так и среду, в которой она работает. Эти сотрудники должны быть выбраны из широкого круга представителей организации, в том числе из:

a) высшего руководства (например, главный инженер и финансовый директор);

b) членов Комитета по информационной безопасности;

c) членов Группы планирования информационной безопасности;

d) руководителей структурных подразделений;

e) владельцев процесса (то есть представители важных производственных участков);

f) специалистов и внешних консультантов.

Информационная безопасность - широкая область, оказывающая влияние на всю организацию. Четкое определение ответственности в области информационной безопасности является фактически очень существенным фактором успешного внедрения СУИБ. Так как роли и ответственность в области информационной безопасности могут изменяться/отличаться, то понимание различных ролей является основой для понимания некоторых видов деятельности, описанных в настоящем стандарте ниже. В таблице B.1 приведена взаимосвязь ролей и ответственности в области информационной безопасности. Необходимо отметить, что в таблице B.1 приведены общие описания ролей, а для каждой конкретной СУИБ необходимы конкретные описания.

Таблица B.1 – Перечень примерных ролей и ответственности в области информационной безопасности

Роли	Краткое описание ответственности
Высшее руководство (например, главный инженер, генеральный директор, начальник службы информационной безопасности, финансовый директор)	Отвечает за концепцию, стратегические решения и координацию деятельности по руководству и контролю организации
Руководители структурных подразделений	Несут высокую ответственность за выполнение функций организации
Директор по информационной безопасности	Несет общую ответственность и руководит обеспечением информационной безопасности, гарантирующим правильную обработку информационных активов

Продолжение таблицы В.1

Роли	Краткое описание ответственности
Комитет по информационной безопасности (члены)	Обрабатывает информационные активы и играет главную роль в СУИБ организации
Группа планирования информационной безопасности (члены)	Работает только во время внедрения СУИБ. Группа планирования взаимодействует со всеми подразделениями и разрешает возникающие противоречия между ними во время внедрения СУИБ
Заинтересованные стороны	В контексте описания других ролей в области информационной безопасности, роль «заинтересованные стороны» в настоящем стандарте определяется главным образом как лица/органы, не участвующие в нормальной работе организации, например, правление, владельцы (организации-владельцы, если организация является частью группы или государственной организации, и/или непосредственные владельцы, например, акционеры частной компании). Другими примерами заинтересованных сторон могут быть дочерние компании, клиенты, поставщики или многочисленные общественные организации, например, агентства по государственному финансовому контролю или соответствующая фондовая биржа, участником которой является организация
Системный администратор	Отвечает за информационную систему
Начальник службы информационных технологий	Управляет всеми ресурсами информационных технологий (например, начальник подразделения информационных технологий)
Физическая безопасность	Лицо, отвечающее за физическую безопасность, например, зданий и т.п., зачастую называемое управляющим инфраструктурой организации или начальником общего отдела
Управление рисками	Лицо/лица, отвечающие в организации за управление рисками, в том числе за оценку, обработку и мониторинг рисков
Юрисконсульт	Несет ответственность за принятие во внимание юридических аспектов множества рисков информационной безопасности
Отдел кадров	Лицо/лица, несущие полную ответственность за персонал
Архив	Все организации имеют архивы, содержащие жизненно важную информацию, которую необходимо хранить в течение длительного времени. Информация может находиться на различных типах носителей, и должен быть выделен отдельный со-

Окончание таблицы В.1

Роли	Краткое описание ответственности
	трудник, ответственный за безопасность хранения этой информации
Персональные данные	Если того требуют законы государства, то может быть назначен сотрудник, отвечающий за взаимодействие с органом, осуществляющим проверку данных, или с аналогичной официальной организацией, которая ведает вопросами сохранения целостности и секретности персональных данных
Разработчик систем	Лицо, отвечающее за разработку собственных информационных систем организации
Специалист/эксперт	Лица, ответственные за некоторые области деятельности организации, привлекаемые к решению некоторых вопросов относительно СУИБ, если эти вопросы относятся к их областям деятельности
Внешний консультант	Лица, не являющиеся сотрудниками данной организации, которые могут дать рекомендации, основанные на объективной оценке ими ситуации в организации и их опыте работы. Однако консультанты обычно не обладают глубокими знаниями об организации и ее деятельности
Сотрудник/персонал/пользователь	Несут равную ответственность за обеспечение информационной безопасности на своих рабочих местах и их окружающей среде
Аудитор	Лицо, отвечающее за оценку СУИБ
Преподаватель	Лицо, реализующее программы повышения осведомленности и тренингов
Ответственные за информационные технологии или информационную безопасность на рабочих местах	Сотрудники крупной организации, назначенные ответственными на рабочих местах по вопросам информационных технологий и, возможно, также за информационную безопасность
Куратор (влиятельное лицо)	Лицо, фактически не играющее ответственную роль, но в большой организации это лицо может оказать существенную помощь на этапе внедрения СУИБ, так как оно обладает глубокими знаниями в этой области и может оказать поддержку в понимании и обосновании внедрения СУИБ. Это лицо может положительно влиять на мнение относительно внедрения СУИБ и его также можно назвать «полномочный представитель администрации»

Приложение С
(справочное)

Внутренний аудит

В этом приложении содержатся дополнительные рекомендации по планированию аудита.

После внедрения СУИБ через определенные интервалы времени должна производиться ее регулярная оценка посредством проведения внутренних и независимых аудитов. Целью аудитов также является упорядочение и оценка опыта, получаемого в повседневной практике. Для внедренной СУИБ необходимо планировать формы аудита.

Полученные результаты аудита СУИБ должны подтверждаться доказательствами. Следовательно, для сбора необходимых доказательств должно быть выделено некоторое соответствующее время в период функционирования СУИБ.

Внутренний аудит СУИБ должен выполняться регулярно, во время его проведения должно проверяться соответствие целей и средств управления, процессов и процедур СУИБ требованиям O‘z DSt ISO/IEC 27001 и соответствующих законодательных или нормативных актов, соответствуют ли они определенным требованиям в области информационной безопасности, а также эффективны ли их внедрение и эксплуатация.

Однако, для небольших компаний выбор внутренних аудиторов СУИБ может стать затруднительным. Если среди персонала отсутствуют опытные сотрудники, способные провести внутренний аудит, то следует привлечь сторонних экспертов. В этом случае необходимо учесть следующее: внешние аудиторы хорошо знакомы с процедурами внутренних аудитов СУИБ; однако они не обладают достаточными знаниями о внутренней и внешней среде организации. Эта информация должна быть предоставлена им персоналом организации. С другой стороны, внутренние аудиторы могут выполнить детальные аудиты внутренней и внешней среды организации, но они не имеют достаточных знаний для выполнения аудитов СУИБ. Организации при выполнении внутренних аудитов СУИБ должны учитывать характеристики и потенциальные недостатки как внутренних, так и внешних аудиторов.

При проведении внутренних аудитов должны быть проверены эффективность и результативность установленных средств управления в соответствии с O‘z DSt ISO/IEC 27004.

Важно, чтобы в этих аудитах не участвовали те лица, которые занимались планированием и разработкой целей безопасности, поскольку им будет затруднительно найти свои собственные ошибки. Следовательно, руководство организации в качестве аудиторов должно привлекать подразделения или сотрудников, которые не входят в область действия

внутренних аудитов СУИБ. Эти аудиторы должны планировать, проводить, следить за проведением внутренних аудитов СУИБ, составлять отчеты об их результатах в соответствии с полученными распоряжениями руководства. В небольшой организации во избежание возникновения такой ситуации, когда сотрудники не смогут выполнять свою собственную работу, вероятно полезно пригласить внешних аудиторов.

При проведении внутреннего аудита СУИБ должно быть проверено, что СУИБ эффективно функционирует и эксплуатируется должным образом. При планировании программы аудита аудиторы должны принять во внимание состояние и важность целей и средств управления, процессов и процедур, подлежащих аудиту, а также результаты предшествующих аудитов.

При проведении аудита должны быть задокументированы критерии, предполагаемая область действия, частота и метод аудита.

Выбранные аудиторы должны обеспечить объективность и беспристрастность процесса аудита. Для проведения серии процессов аудита необходимо, чтобы аудиторы были компетентны в следующих областях:

a) планирование и проведение аудита;

b) отчетность по результатам аудита;

c) рекомендации по корректирующим и предупреждающим действиям, и т.п.

Кроме того необходимо, чтобы в организации были определены и задокументированы ответственность аудиторов и серия процессов аудита.

Руководитель, ответственный за процесс аудита, должен обеспечить, чтобы несоответствия и их причины устранялись без задержки соответствующим образом. Однако это не означает, что несоответствия обязательно должны быть устранены немедленно. Кроме того, выполнение корректирующих действий должно включать их проверку и отчет по результатам проверки.

Внутренний аудит СУИБ может эффективно выполняться как одновременно с проведением других видов внутреннего аудита организации, так и отдельно от них. При проведении аудита рекомендуется пользоваться стандартом O‘z DSt ISO/IEC 27006.

Приложение D
(справочное)

Структура политик

Данное приложение содержит дополнительные рекомендации по структуре политик, в том числе политики информационной безопасности.

Как правило, политика – это документальное подтверждение общей цели и директив, формально выраженных руководством. Политика содержит рекомендации относительно действий и решений, касающихся предмета политики. Организация может иметь несколько политик; для каждой сферы деятельности, важной для организации. Некоторые политики независимы друг от друга, тогда как другие политики имеют иерархическую взаимосвязь. В области безопасности политики, как правило, организуются иерархически. Обычно политика безопасности организации является политикой самого высокого уровня. Она дополняется несколькими более конкретными политиками, в том числе политикой информационной безопасности и политикой системы управления информационной безопасностью. В свою очередь политика информационной безопасности может быть дополнена множеством более подробных политик относительно аспектов информационной безопасности. Многие из этих политик описаны в O‘z DSt ISO/IEC 27002, например, политика информационной безопасности дополняется политикой управления доступом, политиками «чистого стола» и «чистого экрана», использования сетевых служб и использования криптографических средств управления. В некоторых случаях возможно добавление дополнительных уровней политик. Взаимосвязь политик показана на рисунке D.1.

В соответствии с требованиями стандартов O‘z DSt ISO/IEC 27001 и O‘z DSt ISO/IEC 27002 организации необходимо иметь как политику СУИБ, так и политику информационной безопасности. Однако в этих стандартах не определена какая-либо особая взаимосвязь между этими политиками. Требования к политике СУИБ приведены в 4.2.1 O‘z DSt ISO/IEC 27001. Рекомендации относительно политики информационной безопасности приведены в 5.1.1 O‘z DSt ISO/IEC 27002. Эти политики могут разрабатываться как независимые политики или политика СУИБ может подчиняться политике информационной безопасности и наоборот.

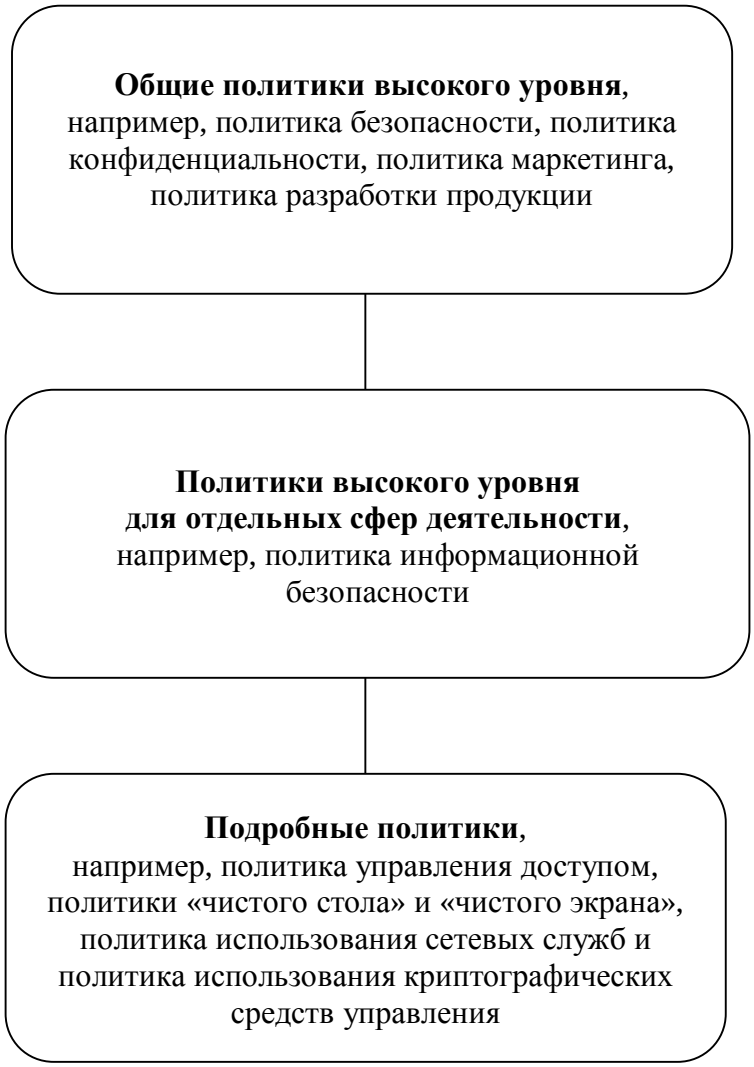


Рисунок D.1 - Иерархия политик

Содержание политик основывается на контексте деятельности организации. При разработке любой политики в ее содержании должно быть отражено следующее (рисунок D.2) :

1) цели и задачи организации;
2) стратегии достижения этих целей;
3) структура организации и применяемые процессы;
4) цели и задачи, связанные с предметом политики;
5) требования политик более высокого уровня.

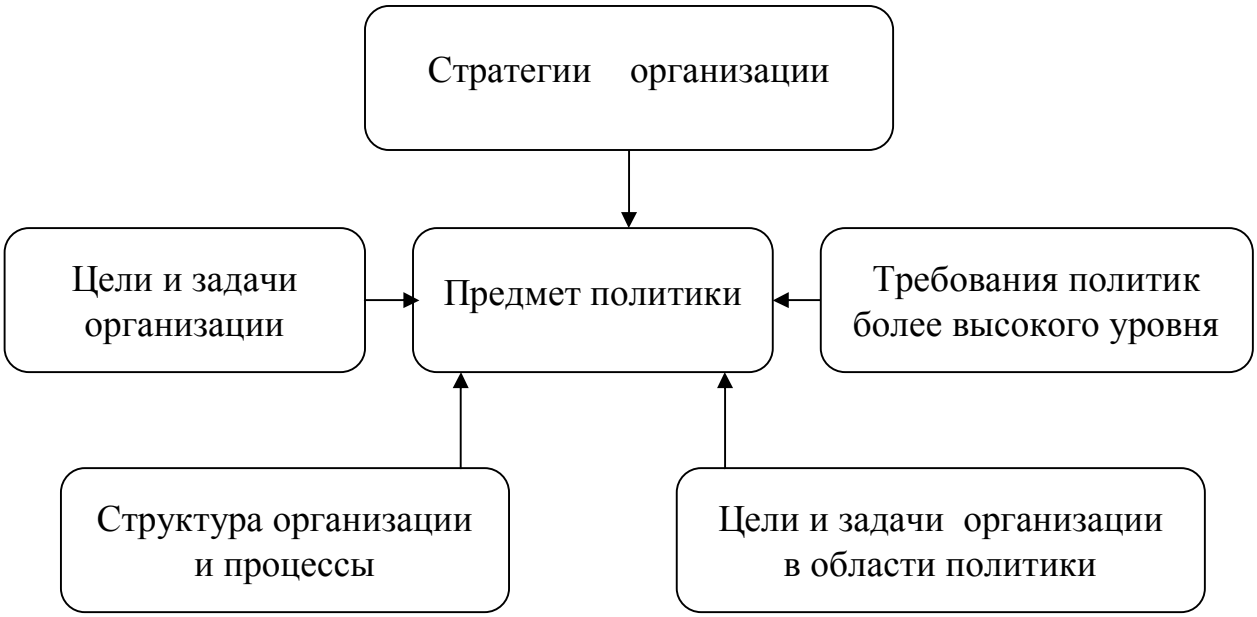


Рисунок D.2 - Исходные данные для разработки политики

Политики могут иметь следующую структуру:

1) аннотация политики – краткое описание политики, состоящее из одного или двух предложений (иногда может объединяться с введением);

2) введение - краткое разъяснение предмета политики;

3) область действия - описание тех подразделений организации или ее видов деятельности, на которые распространяется политика. При необходимости в разделе «Область действия» делаются ссылки на другие политики, дополняемые этой политикой;

4) цели - описание предназначения политики;

5) принципы – описание правил относительно действий и решений по достижению целей. В некоторых случаях может быть полезно определить ключевые процессы, связанные с предметом политики, а затем правила выполнения процессов;

6) ответственность - описание того, кто отвечает за выполнение требований политики. В некоторых случаях этот раздел может включать описание организационной структуры, а также ответственности лиц с определенными ролями;

7) основные результаты - описание результатов деятельности организации при достижении целей.

8) взаимосвязь с другими политиками – описание других политик, необходимых для достижения целей, обычно содержащее дополнительные подробности относительно конкретных предметов.

Примечание – Содержание политик может различаться. Например, организации, уделяющие особое внимание ролям и ответственности, могут упростить описание целей, а конкретные принципы и ответственность описать в одном разделе.

Ниже приведены примерные структура и содержание политики информационной безопасности.

Политика информационной безопасности (пример)

Аннотация политики

Информация вне зависимости от ее формы представления и способов распространения, обмена или хранения должна быть всегда надлежащим образом защищена.

Введение

Информация может существовать во многих формах. Она может быть напечатана или написана на бумаге, храниться в электронном виде, посылаться по почте или передаваться с помощью электронных средств, записываться на пленках или устно передаваться в разговоре.

Информационная безопасность – это защита информации от большого разнообразия угроз, осуществляемая с целью обеспечения непрерывности бизнеса, минимизации бизнес-рисков, а также максимизации возврата по инвестициям и возможностей бизнес-деятельности.

Область действия

Настоящая политика поддерживает общую политику безопасности организации.

Настоящая политика распространяется на всю организацию.

Цели информационной безопасности

1) Осознание существования в организации стратегических и операционных рисков информационной безопасности и их обработка до приемлемого уровня.

2) Обеспечение конфиденциальности информации о клиентах, защита разработок продукции и маркетинговых планов.

3) Сохранение целостности данных бухгалтерского учета.

4) Соответствие общедоступных веб-служб и внутренних сетей требованиям соответствующих стандартов доступности.

Принципы информационной безопасности

1) Организация способствует принятию рисков и допускает риски, которые недопустимы в консервативно управляемых организациях, при условии, что информационные риски будут осознаны, контролируемы и при необходимости обработаны. Подробное описание метода, применяемого для определения и обработки рисков, содержится в политике СУИБ.

2) Весь персонал будет осведомлен и подотчетен в области информационной безопасности в соответствии со своими должностными обязанностями.

3) На эксплуатацию средств управления информационной безопасностью и процессы управления проектами будет открыто финансирование.

4) При общем управлении информационными системами необходимо учесть возможность мошенничества, связанного со злоупотреблением ими.

5) Отчеты о состоянии информационной безопасности будут доступны.

6) Риски информационной безопасности будут контролироваться, а когда результаты изменений рисков станут неприемлемыми, будут предприняты соответствующие действия.

7) Критерии классификации и приемлемости рисков приведены в политике СУИБ.

8) Организация не допустит возникновения ситуаций, при которых не будут соблюдаться требования нормативно-правовых актов.

Ответственность

1) Высшее руководство отвечает за обеспечение адекватного рассмотрения информационной безопасности во всей организации.

2) Каждый руководитель подразделения отвечает за то, что работающие в его подразделении сотрудники осуществляют защиту информации в соответствии со стандартами организации.

3) Начальник отдела обеспечения информационной безопасности консультирует высшее руководство, оказывает квалифицированную помощь персоналу организации и обеспечивает доступность отчетов о состоянии информационной безопасности.

4) Каждый сотрудник организации отвечает за информационную безопасность в соответствии со своими должностными обязанностями.

Основные результаты

1) Инциденты информационной безопасности не повлекут за собой значительных и непредвиденных расходов или продолжительного прекращения работы служб и бизнес-деятельности.

2) Убытки от мошенничества известны и находятся в приемлемых пределах.

3) Клиенты, получающие продукты или услуги, не будут беспокоиться относительно информационной безопасности.

Взаимосвязь с другими политиками

Подробные описания принципов и рекомендаций по отдельным аспектам информационной безопасности содержатся в нижеперечисленных политиках:

1) политика СУИБ;

2) политика управления доступом;

3) политика «чистого стола» и «чистого экрана»;

4) политика ограничения использования неавторизованного программного обеспечения;

5) политика получения файлов программного обеспечения из внешних сетей или через них;

6) политика использования мобильных кодов;

7) политика резервного копирования;

8) политика обмена информацией между организациями;

9) политика допустимого использования электронных средств связи;

10) политика хранения записей;

11) политика использования сетевых служб;

12) политика использования мобильных компьютеров и мобильной связи;

13) политика работы в дистанционном режиме;

14) политика использования криптографических средств защиты информации;

15) политика контроля соответствия требованиям международных стандартов и внутренним политикам организации в области информационной безопасности;

16) политика лицензирования программного обеспечения;

17) политика удаления программного обеспечения;

18) политика защиты данных и политика приватности.

Все эти политики поддерживают:

- идентификацию рисков путем предоставления базовых средств управления, которые могут быть использованы для выявления недостатков, допущенных при проектировании и внедрении систем;

- обработку рисков путем определения способов их обработки для идентифицированных уязвимостей и угроз.

Процессы «идентификация рисков» и «обработка рисков» определены в разделе «Принципы информационной безопасности».

Приложение Е
(справочное)

Мониторинг и измерения

В данном приложении приведены дополнительные рекомендации, которые помогут при планировании и разработке мониторинга и измерений.

Информация по настройке мониторинга и измерений

Разработка специфических требований к СУИБ включает разработку программы мониторинга и измерений безопасности для СУИБ, которая необходима для организации анализа со стороны руководства.

Разработка мониторинга

Последовательность процесса мониторинга показана на рисунке Е.1.

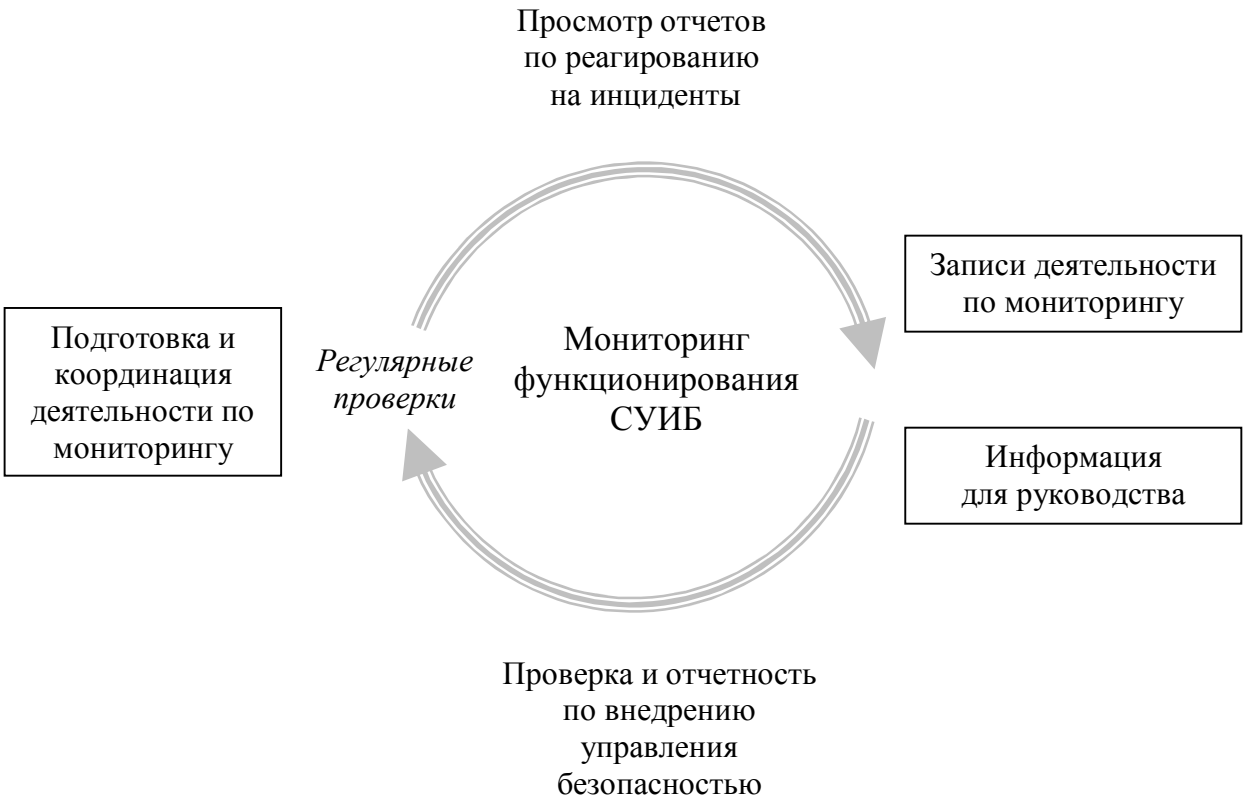


Рисунок Е.1 – Последовательность процесса мониторинга

Подготовка и координация: определение активов, подлежащих мониторингу

Необходимо отметить, что мониторинг является непрерывным процессом; при его разработке должна быть учтена настройка процесса мониторинга, а также разработка фактической потребности в мониторинге и деятельности по мониторингу. Координация этой деятельности является обязательной частью разработки.

Цели мониторинга могут быть определены на основе ранее определенной совокупности данных об области действия и активах в сочетании с результатами анализа рисков и выбора средств управления. Эти цели должны включать ответы на следующие вопросы:

- что необходимо обнаружить;
- когда;
- относительно чего.

На практике заблаговременно установленные виды деятельности/процессы организации и связанные с ними активы являются основной областью действия мониторинга (будет получен ответ на вопрос «относительно чего»). При разработке мониторинга возможно потребуется выбрать важные, с точки зрения информационной безопасности, активы. Также при определении того, что должно быть проверено в активах и связанных с ними видах деятельности/процессах организации, следует принять во внимание результаты обработки рисков и выбора средств управления (Это даст ответ на вопросы «что необходимо обнаружить» и «когда»).

Учитывая, что при проведении мониторинга могут иметь место юридические аспекты, то разработка мониторинга должна быть непременно проверена, чтобы при проведении мониторинга не было каких-либо юридических последствий.

Для обеспечения действительной эффективности мониторинга важное значение имеет обязательная координация и выполнение всех видов деятельности при окончательной разработке мониторинга.

Деятельность по мониторингу

Для поддержания необходимого уровня информационной безопасности средства управления информационной безопасностью, определенные как подходящие, должны использоваться правильно; обнаружение инцидентов безопасности и реагирование на них должны производиться своевременно, а функционирование СУИБ должно регулярно проверяться. Чтобы убедиться в том, что все имеющиеся в наличии средства управления, внедренные в соответствии с концепцией информационной безопасности, используются, необходимо проводить регулярные проверки.

Эти проверки должны включать проверку соответствия технических средств управления (например, конфигурации) и организационных средств управления (например, процессов, процедур и операций). Прежде всего

проверки должны быть направлены на устранение недостатков. Важно, чтобы все вовлеченные сотрудники понимали цель проверок – утверждение их результатов. Во время проверок необходимо обсуждать возможные решения проблем с участниками и предварительно найти соответствующие способы устранения недостатков.

Чтобы проверки прошли как можно более эффективно и чтобы одновременно при этом было как можно меньше нарушений обычной работы организации, проверки должны быть тщательно подготовлены. Общее проведение проверок должно быть заранее согласовано с руководством. Деятельность по мониторингу может включать три разные основные формы:

- отчеты об инцидентах;
- подтверждение соответствия или несоответствия функционального назначения средств управления;
- другие регулярные проверки.

Далее необходимо будет разработать форму представления результатов деятельности по мониторингу, то есть как должны быть выполнены записи и как должна быть представлена руководству информация. В документации, выполненной по установленной форме, должны быть описаны разработка мониторинга, принципы и цели деятельности по мониторингу, а также различные сферы ответственности.

Требования к результатам мониторинга

Результатами мониторинга должны быть:

a) записи деятельности по мониторингу с необходимым уровнем детализации.

По результатам деятельности по мониторингу руководству должен быть представлен отчет. Этот отчет должен содержать всю информацию, необходимую руководству для выполнения своих управленческих и контролирующих функций, записанную с необходимым уровнем детализации;

b) информация, которая потребуется руководству для принятия решения в случае необходимости оперативных действий.

Отчет руководству должен во всех случаях заканчиваться перечнем рекомендуемых действий, с четко определенными приоритетами, вместе с реальной оценкой предполагаемых затрат на реализацию каждого из этих действий. Это позволит руководству незамедлительно принять решения.

Установка программы измерения информационной безопасности.

Обзор разработки программы измерения информационной безопасности

Процесс измерения должен быть эффективно интегрирован в цикл проекта СУИБ или организации и использоваться для непрерывного улучшения процессов, связанных с безопасностью, и результатов этого проекта или организации. Согласно O‘z DSt ISO/IEC 27004 этот процесс называется программой измерения информационной безопасности.

Разработку программы необходимо рассматривать с точки зрения цикла СУИБ. На рисунке Е.2 показано, как процесс измерения встраивается в цикл СУИБ.

Рисунок Е.2 - Два аспекта измерения эффективности СУИБ с помощью процесса PDCA и примеры процессов внутри организации

Для выполнения заданных требований и получения ожидаемых результатов системы управления должны выполнять следующие функции: структурирование, необходимое для PDCA; измерение выходных данных и подтверждение их эффективности; передача по каналу обратной связи результатов измерения руководителю процессов.

Существенным условием правильного выполнения измерения является использование прежде полученной информации, а именно:

а) политики СУИБ, включая ее область действия и границы;

b) результата определения рисков;

c) выбранных средств управления;

d) целей управления;

e) специфических целей информационной безопасности;

f) заданных процессов и ресурсов, а также их классификации.

Руководство должно принять и выполнять обязательства по всему процессу измерения. При выполнении процесса измерения руководство должно:

a) установить требования к измерениям в соответствии с O‘z DSt ISO/IEC 27004;

b) сосредоточить внимание на получении всей необходимой информации в соответствии с O‘z DSt ISO/IEC 27004;

c) возложить на персонал следующие обязательства:

- организация должна продемонстрировать свои обязательства, например, посредством политики измерений для организации, распределения ответственности и обязанностей, тренингов, распределения бюджета и других ресурсов;

- должно быть назначено лицо или подразделение организации, ответственное за программу измерений;

- должно иметь поддержку руководства лицо или подразделение организации, ответственное за обмен значимыми результатами измерений СУИБ со всеми подразделениями организации, которые должны их получать и использовать;

- проверять выполнение сбора, анализа результатов измерений СУИБ, отчитываться перед руководителем подразделения по информационным технологиям и другими заинтересованными сторонами;

- научить руководителей структурных подразделений использовать результаты программы измерений СУИБ для принятия решений относительно политики, распределения ресурсов и бюджета.

Программа и проект измерения информационной безопасности должны включать следующие роли:

a) высшее руководство;

b) пользователи продуктов безопасности;

c) лица, ответственные за информационные системы;

d) лица, ответственные за информационную безопасность.

Программа измерения информационной безопасности, описанная в O‘z DSt ISO/IEC 27004, используется для получения показателей эффективности СУИБ, целей и средств управления.

Для достижения этих целей необходимо провести соответствующие измерения в фазе планирования.

Используемые программы измерения информационной безопасности могут различаться в зависимости от структуры организаций, а именно:

- размера;

- сложности;

- общего профиля риска/потребности информационной безопасности.

Обычно для большой организации со сложной структурой необходима более обширная программа измерения. На обширность программы измерения также влияет уровень общего риска. Если влияние неэффективной информационной безопасности серьезное, то для сравнительно небольшой организации, чтобы покрыть риски, возможно потребуется более исчерпывающая программа измерения, чем для большой организации, на которую не оказывается такое влияние.

Оценка обширности программы измерения может быть основана на выбранных средствах управления и результатах анализа рисков, которые должны быть покрыты.

Разработка программы измерения информационной безопасности

Лицо, ответственное за программу измерения информационной безопасности, должно учитывать следующее:

- область применения;
- измерения;
- выполнение измерений;
- периодичность измерений;
- отчетность.

Область применения программы измерения должна охватывать область действия, цели и средства управления СУИБ. В частности, цели и границы измерения СУИБ должны быть установлены исходя из характеристик организации, ее местоположения, активов и технологии, а также включать детализацию и обоснования для всех исключений из области действия СУИБ. Это может быть одно из средств управления безопасностью, процесс, система, функциональная область, целое предприятие, одно подразделение или организация, имеющая в своем составе несколько подразделений.

Согласно O‘z DSt ISO/IEC 27004 начальной точкой при выборе каждого отдельного измерения должен быть объект измерения. Для установления программы измерения должны быть определены эти объекты. Объектами измерений могут быть процессы или ресурсы. При установлении программы объекты, находящиеся в области действия СУИБ, во многих случаях разделяются на части для того, чтобы найти фактически существующие объекты, которые необходимо измерить. Этот процесс определения объектов можно пояснить следующим образом:

- организация является комплексным объектом;
- процесс А или информационная система Х организации является частью этого комплексного объекта и по своей сути тоже является объектом;
- объекты в рамках этого процесса, влияющие на информационную безопасность (персонал, правила, сеть, приложения, аппаратные средства и т.п.) обычно являются объектами измерения, позволяющими увидеть эффективность защиты информации.

При выполнении программы измерения информационной безопасности необходимо иметь в виду, что объекты измерения могут служить для выполнения многих процессов в организации в пределах области действия СУИБ и могут, следовательно, оказывать большое влияние на эффективность СУИБ и цели управления. Такие объекты обычно получают приоритет в области действия программы, например, безопасность организации и связанные с ней процессы, компьютерный зал, сотрудники, имеющие отношение к информационной безопасности, и т.п.

Периодичность измерений может меняться, но предпочтительнее, чтобы через определенные промежутки времени измерения выполнялись или обобщались для анализа со стороны руководства и непрерывного процесса улучшения и поддержания СУИБ. Это необходимо учесть при разработке программы.

Отчетность по результатам измерений должна быть разработана таким образом, чтобы представление информации производилось согласно O‘z DSt ISO/IEC 27004.

Процедура разработки программы измерения информационной безопасности должна быть задокументирована и утверждена руководством. В этом документе должно быть отражено следующее:

a) ответственность за программу измерения информационной безопасности;

b) ответственность за представление информации;

c) область применения измерений;

d) как и кем должна выполняться программа (основной используемый метод, персоналом своей или сторонней организации и т.п.);

e) когда должна выполняться программа;

f) способы представления отчетности.

Если организация разрабатывает свои собственные точки измерения, то это должно быть задокументировано как часть фазы проекта в соответствии с O‘z DSt ISO/IEC 27004. Этот документ может быть очень большим и его не обязательно подписывать у руководства, так как в него при выполнении измерений могут вноситься изменения.

Измерение эффективности СУИБ

При определении области применения программы измерения информационной безопасности, которая должна быть внедрена, необходимо сделать так, чтобы не было слишком много объектов. В противном случае представляется разумным разделить программу на разные части. Область действия этих частей может быть представлена отдельными измерениями для сравнения, но преобладает их основная цель: использование совокупности измерений в качестве показателя для оценки эффективности СУИБ. Эти подобласти обычно являются подразделениями организации, у которых могут быть определены четкие границы. Совокупность объектов, которые служат для выполнения многих процессов организации, и измерения объектов в границах этих подобластей могут вместе образовать

соответствующую область применения программы измерения информационной безопасности. Эту совокупность также можно представить как ряд деятельностей СУИБ, который состоит из двух или более процессов/объектов. Следовательно, измерение эффективности всей СУИБ может быть основано на результатах измерения этих двух или более процессов/объектов.

С учетом того, что целью является измерение эффективности СУИБ, важно измерить цели и средства управления. Одним аспектом является достаточное количество средств управления, а другим аспектом – то, что этих средств управления достаточно для оценки эффективности СУИБ (рисунок Е.2). Область применения программы измерения информационной безопасности может быть ограничена другими причинами, рассматриваемыми в O‘z DSt ISO/IEC 27004.

При использовании результатов измерения для оценки эффективности СУИБ, целей и средств управления существенным условием является осведомленность руководства об области действия программы измерения информационной безопасности. Лицо, ответственное за программу измерения, должно получить у руководства разрешение на область применения программы измерения информационной безопасности до внедрения этой программы.

Примечания

1 Выполняется измерение эффективности средств управления или группы средств управления.

2 Необходим только анализ эффективности всей СУИБ, измерение всей СУИБ не требуется.

Фактически измерения могут выполняться персоналом как своей или сторонней организации, так и совместно. Размер, структура организации и ее организационная культура являются факторами, которые необходимо учитывать при оценке внутренних или внешних ресурсов. Компаниям небольшого и среднего размера выгоднее использовать сторонних специалистов, чем большим организациям. Результаты использования внешних ресурсов, в зависимости от организационной культуры, могут также обеспечить более достоверный результат. Если в организации регулярно проводятся внутренние аудиты, результаты использования внутренних ресурсов могут быть точно также достоверны.

Приложение F
(справочное)

Примеры критических факторов успеха

Примерами критических факторов успеха являются:

a) политика информационной безопасности, цели и деятельность, направленные на достижение целей;

b) методика и инфраструктура, необходимые для проектирования, внедрения, мониторинга, эксплуатации и улучшения информационной безопасности, соответствующие организационной культуре;

c) ощутимая поддержка и обязательства со стороны всех уровней управления, особенно высшего руководства;

d) понимание требований защиты информационных активов, достигаемое посредством управления рисками информационной безопасности в соответствии с O‘z DSt ISO/IEC 27005;

e) степень осведомленности в области информационной безопасности, тренинги и обучающие программы, информирование всех служащих и других соответствующих сторон об их обязательствах в области информационной безопасности, изложенных в политиках информационной безопасности, стандартах и т.п., и их мотивация к соответствующим действиям;

f) эффективный процесс управления инцидентами информационной безопасности;

g) эффективный метод управления непрерывностью бизнеса;

h) система измерений, используемая для оценки выполнения управления информационной безопасностью и выдачи предложений по его улучшению.

Приложение G
(справочное)

Сведения о соответствии государственных стандартов Узбекистана международным стандартам

Таблица G.1

Обозначение и наименование ссылочного государственного стандарта Узбекистана	Степень соответствия	Обозначение и наименование соответствующего международного стандарта
O‘z DSt ISO/IEC 27000:2014 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь	MOD	ISO/IEC 27000:2014 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь
O‘z DSt ISO/IEC 27001:2009 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования	IDT	ISO/IEC 27001:2005 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования
O‘z DSt ISO/IEC 27002:2008 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью	IDT	ISO/IEC 27002:2005 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью.
O‘z DSt ISO/IEC 27004:2014 Информационная технология. Методы обеспечения безопасности. Измерение эффективности системы управления информационной безопасностью	MOD	ISO/IEC 27004:2009 Информационная технология. Методы обеспечения безопасности. Управление информационной безопасностью. Измерения
O‘z DSt ISO/IEC 27005:2013 Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности	MOD	ISO/IEC 27005:2011 Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности
O‘z DSt ISO/IEC 27006:2013 Информационная технология. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью	MOD	ISO/IEC 27006:2007 Информационная технология. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью
Примечание – В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов: IDT - идентичная; MOD – модифицированная.		

Приложение H

(справочное)

Технические отклонения и объяснение причин их внесения

H.1 В стандарт включены следующие редакционные изменения: слова «данный международный стандарт» заменены на «настоящий стандарт».

H.2 Стандарт оформлен с учетом требований O‘z DSt 1.6:2003.

H.3 В стандарт включены отдельные изменения и дополнения. Перечень внесенных модификаций и объяснение причин их внесения приведены в таблице H.1.

Таблица H.1 – Перечень внесенных модификаций

Раздел	Модификация	Объяснение
Предисловие	Исключено	В связи с тем, что предисловие содержит информацию только о разработке международного стандарта
Раздел 2	Международный стандарт ISO/IEC 27001:2005 заменен на O‘z DSt ISO/IEC 27001:2009	В соответствии с приложением G
	Включены государственные стандарты Узбекистана: - O‘z DSt ISO 9001:2009; - O‘z DSt ISO 14001:2009; - O‘z DSt ISO/IEC 27002:2008; - O‘z DSt ISO/IEC 27004:2014; - O‘z DSt ISO/IEC 27005:2013; - O‘z DSt ISO/IEC 27006:2013	В связи с исключением библиографии. Соответствующие международные стандарты заменены на государственные стандарты Узбекистана в соответствии с приложением G
4.1, перечень приложений	Дополнен приложением F	В связи с исключением ссылки на стандарт ISO/IEC 27000:2009 в 5.4
5.2, дополнительная информация	Исключена ссылка на международный стандарт ISO/IEC 20000-1:2005	В связи с тем, что указанный стандарт на территории Республики Узбекистан не действует
5.4, дополнительная информация	Исключена ссылка на международный стандарт ISO/IEC 27000:2009, изменена редакция	Добавлено приложение F
Приложения	Добавлено приложение F «Примеры критических факторов успеха»	В связи с исключением ссылки на стандарт ISO/IEC 27000:2009 в 5.4

Окончание таблицы Н.1

Раздел	Модификация	Объяснение
Библиография	Исключена	В связи с тем, что международные стандарты, имеющие соответствующие государственные стандарты Узбекистана, перенесены в раздел 2. На остальные международные стандарты ссылки в тексте международного стандарта отсутствуют.

УДК 681.324:006.354 ОКС 35.040 Т55

Ключевые слова: информационная технология, система управления информационной безопасностью, область действия, определение и обработка рисков, цели и средства управления, политика информационной безопасности

Вр.и.о. директора
ГУП «UNICON.UZ» Х. Хасанов

Начальник научно-
исследовательского отдела
криптографии О. Ахмедова

Ведущий инженер
научно-исследовательского отдела
криптографии С. Абрамова

Младший научный сотрудник
научно-исследовательского отдела
криптографии Д. Джаматова

Нормоконтроль Л. Шаймарданова

СОГЛАСОВАНО

Начальник отдела
информационной безопасности
Государственного комитета связи,
информатизации и телекоммуникационных
технологий Республики Узбекистан

А. Гафуров
письмо от 04.02.2013
№ 14-8/414

СОГЛАСОВАНО

Первый заместитель начальника
Государственной инспекции по надзору
в сфере связи информатизации и
телекоммуникационных технологий

А. Гафуров
письмо от 28.12.2012
№ 32-12/1596