

Отчёт по проектной деятельности:

«Анализ подходов к оценке зрелости процессов информационной безопасности на основе зарубежных фреймворков».

Студент 2 курса

факультета Информационных технологий

группы 191-331

Горшков А.Г.

Научный руководитель:

Агеева Елена Александровна

ОГЛАВЛЕНИЕ

Введение . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 3

Описание . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .4

Краткая выписка . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .6

Этап 2. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .10

Стандарты . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .27

Заключение . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .32

ВВЕДЕНИЕ

Моим проектом было рассмотрение ГОСТ Р ИСО/МЭК 27001-2006(далее ГОСТ). Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности требования.

Было довольно сложно правильно подойти к этому заданию, т.к. анализ ГОСТа с целью выявления рисков Информационной Безопасности(далее ИБ) в иностранных компаниях подразумевает выявления основных частей ГОСТА, и анализ уязвимостей в компании. В самом ГОСТе все части являются основными, ведь ГОСТ сам является выпиской с основополагающими понятиями.

Моя работа представляет собой кратко сформированный анализ самого ГОСТа и компаний, которые могут быть подвержены рискам ИБ связанных с ним.

Также в мою работу включён анализ подхода к рискам ИБ непосредственно в самом ГОСТе.

ОПИСАНИЕ

Как сказано в предисловии:

“ПОДГОТОВЛЕН Федеральным государственным учреждением "Государственный научно-исследовательский испытательный институт проблем технической защиты информации Федеральной службы по техническому и экспортному контролю" (ФГУ "ГНИИИ ПТЗИ ФСТЭК России") и Обществом с ограниченной ответственностью "Научно-производственная фирма "Кристалл" (ООО "НПФ "Кристалл") на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте -

Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27001:2005\* "Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования" (ISO/IEC 27001:2005 "Information technology - Security techniques - Information security management systems - Requirements", IDT)”.

В данном стандарте достаточно точно и чётко указаны все, на мой взгляд, требования в данной области, которые необходимо рассмотреть.

Настоящий стандарт состоит из нескольких частей:

-Введение

-Текст ГОСТа

-Приложение A

-Приложение B

-Приложение C

Основная информация из введения – это то, что в данном стандарте будет рассматриваться система менеджмента информационной безопасности на основе модели PDCA:

“В настоящем стандарте представлена модель "Планирование (Plan) - Осуществление (Do) - Проверка (Check) - Действие (Act)" (PDCA), которая может быть применена при структурировании всех процессов СМИБ”.

Сам текст ГОСТа состоит из 8 частей, здесь выделить что-то основное довольно трудно, т.к. все части настоящего стандарта являются основополагающими.

В приложении A рассмотрены меры управления (рекомендации), которые тоже необходимы в рассмотрении, т.к. они непосредственно говорят о том, какими действиями какие риски можно избежать или снизить.

В приложении B рассмотрены принципы Организации экономического сотрудничества и развития, их тоже необходимо учесть при формировании системы менеджмента информационной безопасности.

В приложении C рассмотрены сравнения структуры настоящего стандарта со структурой международных компаний. То есть представлена разница между непосредственным стандартом ISO 27001:2005 и этим ГОСТом. В начале указано, что принципиальной разницы между настоящим стандартом ГОСТ и соответствующим ему стандартом ISO нет, но тем не менее небольшие различия имеются. Именно они и рассмотрены в этом приложении.

Данный ГОСТ является весьма “объёмным” и для его введения компания должна обладать весьма неплохими информационными активами и хорошей осведомлённостью в этой сфере, также большими финансовыми ресурсами, т.к. введение, рассмотренной в ГОСТЕ системы требует больших вложений.

В настоящем стандарте реализован профессиональный подход к рискам в области ИБ. Полностью изучены возможные риски в той мере, в какой это возможно на данный момент, и изложена вся суть реализации СМИБ (системы менеджмента информационной безопасности). Но тем не менее, проблема, как и в любой сфере, не сформирована на 100% и развивается каждый день. Поэтому как и любой стандарт ISO 27001 требует «непрерывного улучшения»: систематического исправления и предотвращения несоответствий в системе управления информационной безопасностью. С помощью корректирующих и превентивных действий можно исправить несоответствие и предотвратить его повторное появление в будущем.

Если говорить о сертификации, то на самом деле пройти её намного сложнее, чем это описано в различных источниках. Подтверждением является тот факт, что в России на сегодняшний день всего 78 компаний прошли сертификацию на соответствие. При этом за рубежом это один из наиболее популярных стандартов, отвечающих растущим запросам бизнеса в области ИБ. Такая востребованность внедрения обусловлена не только ростом и усложнением типов угроз, но и требованиями законодательства, а также клиентов, которым необходимо сохранение полной конфиденциальности их данных.  
  
Несмотря на то, что сертификация СМИБ является непростой задачей, сам факт выполнения требований международного стандарта ISO/IEC 27001 может дать серьезное конкурентное преимущество на глобальном рынке.

КРАТКАЯ ВЫПИСКА

Здесь я собрал, на мой взгляд, основные выписки из каждой из глав в содержание настоящего ГОСТа.

Настоящий стандарт предназначен для применения организациями любой формы собственности (например, коммерческими, государственными и некоммерческими организациями). Настоящий стандарт устанавливает требования по разработке, внедрению, функционированию, мониторингу, анализу, поддержке и улучшению документированной системы менеджмента информационной безопасности (СМИБ) среди общих бизнес-рисков организации. Кроме этого, стандарт устанавливает требования по внедрению мер управления информационной безопасностью и ее контроля, которые могут быть использованы организациями или их подразделениями в соответствии с установленными целями и задачами обеспечения информационной безопасности (ИБ).  
  
Целью построения СМИБ является выбор соответствующих мер управления безопасностью, предназначенных для защиты информационных активов и гарантирующих доверие заинтересованных сторон.

Организация должна разработать, внедрить, обеспечить функционирование, вести мониторинг, анализировать, поддерживать и непрерывно улучшать документированную СМИБ применительно ко всей деловой деятельности организации и рискам, с которыми она сталкивается. С учетом целей настоящего стандарта используемый процесс основан на применении модели PDCA.

Разработка СМИБ. Организация должна осуществить следующее:

a) определить область и границы действия СМИБ с учетом характеристик бизнеса, организации, ее размещения, активов и технологий, в том числе детали и обоснование любых исключений из области ее действия;

b) определить политику СМИБ на основе характеристик бизнеса, организации, ее размещения, активов и технологий;

c) определить подход к оценке риска в организации;

d) идентифицировать риски;

e) проанализировать и оценить риски;

f) определить и оценить различные варианты обработки рисков;

g) выбрать цели и меры управления для обработки рисков;

h) получить утверждение руководством предполагаемых остаточных рисков;

i) получить разрешение руководства на внедрение и эксплуатацию СМИБ;

j) подготовить Положение о применимости;

Внедрение СМИБ. Организация должна осуществить следующее:

a) разработать план обработки рисков, определяющий соответствующие действия руководства, ресурсы, обязанности и приоритеты в отношении менеджмента рисков ИБ;

b) реализовать план обработки рисков для достижения намеченных целей управления, включающий в себя вопросы финансирования, а также распределение функций и обязанностей;

c) внедрить меры управления, для достижения целей управления;

d) определить способ измерения результативности выбранных мер управления или их групп и использования этих измерений для оценки результативности управления с целью получить сравнимые и воспроизводимые данные.

e) реализовать программы по обучению и повышению квалификации сотрудников;

f) управлять работой СМИБ;

g) управлять ресурсами СМИБ;

h) внедрить процедуры и другие меры управления, обеспечивающие быстрое обнаружение событий ИБ и реагирование на инциденты, связанные с ИБ.

Документация должна включать в себя записи решений руководства, позволяющие обеспечивать контроль выполнения решений руководства и политик организации, а также обеспечивать воспроизводимость документированных результатов.  
  
Важно иметь обратную связь выбранных мер управления с результатами процессов оценки и обработки риска, а также последних с политикой СМИБ и целями СМИБ.

Для предоставления свидетельств соответствия требованиям и результативности функционирования СМИБ необходимо вести и поддерживать в рабочем состоянии учетные записи. Учетные записи необходимо контролировать и защищать. СМИБ должна принимать во внимание все нормативно-правовые требования и договорные обязательства, имеющие отношение к ИБ. Записи должны быть четкими, легкоидентифицируемыми и восстанавливаемыми. Меры управления, требуемые для идентификации, хранения, защиты, поиска, определения сроков хранения и уничтожения записей должны быть документированы и реализованы.

Руководство организации должно предоставлять доказательства выполнения своих обязательств в отношении разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ путем осуществления следующих мер:

a) разработки политики СМИБ;

b) обеспечения разработки целей и планов СМИБ;

c) определения функций и ответственности в области ИБ;

d) доведения до всех сотрудников организации информации о важности достижения целей информационной безопасности и соответствия ее требованиям политики организации, об их ответственности перед законом, а также о необходимости непрерывного совершенствования в реализации мер ИБ;

e) выделения необходимых и достаточных ресурсов для разработки, внедрения, обеспечения функционирования, мониторинга, анализа, поддержки и улучшения СМИБ;

f) установления критериев принятия рисков и уровней их приемлемости;

g) обеспечения проведения внутренних аудитов СМИБ;

h) проведения анализа СМИБ со стороны руководства.

Организация должна в соответствии с утвержденным графиком проводить внутренние аудиты СМИБ, позволяющие установить, что цели управления, меры управления, процессы и процедуры СМИБ:

a) соответствуют требованиям настоящего стандарта и соответствующим законам или нормативным документам;

b) соответствуют установленным требованиям ИБ;

c) результативно внедряются и поддерживаются;

d) функционируют должным образом.

Руководство должно в соответствии с утвержденным графиком периодически (не менее одного раза в год) проводить анализ СМИБ организации в целях обеспечения ее постоянной пригодности, адекватности и результативности. Результаты анализа должны содержать предложения по изменению СМИБ и оценку их реализации в интересах обеспечения выполнения требований политики и целей информационной безопасности. Результаты таких проверок должны быть зафиксированы документально, а учетные записи должны быть сохранены.

Входные данные для анализа СМИБ со стороны руководства должны включать в себя следующую информацию:

a) результаты предыдущих аудитов и анализа СМИБ;

b) результаты взаимодействия с заинтересованными сторонами;

c) методы, средства или процедуры, которые могут быть использованы в организации для совершенствования функционирования и повышения результативности СМИБ;

d) правовое обоснование предупреждающих и корректирующих действий;

e) уязвимости или угрозы, которые не были адекватно учтены в процессе предыдущей оценки рисков;

f) результаты количественной оценки результативности СМИБ;

g) последующие действия, вытекающие из предыдущего анализа со стороны руководства;

h) любые изменения, которые могли бы повлиять на СМИБ;

i) рекомендации по улучшению.

Организация должна постоянно повышать результативность СМИБ посредством уточнения политики ИБ, целей ИБ, использования результатов аудитов, анализа контролируемых событий, корректирующих и предупреждающих действий, а также использования руководством результатов анализа СМИБ.

Организация должна проводить мероприятия по устранению причин несоответствий требованиям СМИБ с целью предупредить их повторное возникновение. Организация должна определять действия, необходимые для устранения причин потенциальных несоответствий требованиям СМИБ, с целью предотвратить их повторное появление. Предпринимаемые предупреждающие действия должны соответствовать последствиям потенциальных проблем.

Организация должна определить изменения в оценках рисков и установить требования к предупреждающим действиям, при этом обращая особое внимание на существенно измененные количественные показатели рисков.  
  
Приоритеты в отношении реализации предупреждающих действий должны быть определены на основе результатов оценки риска.

**ЭТАП 2**

«Расширенная аналитическая записка с результатами Этапа 1 и описанием процесса оценки процессов ИБ»

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **А.5 Политика безопасности** | | | | | |
| **А.5.1 Политика информационной безопасности**  Цель: Обеспечить участие высшего руководства организации в решении вопросов, связанных с обеспечением информационной безопасности в соответствии с целями деятельности организации (бизнеса), законами и нормативными актами | | | | | |
| A.5.1.1 | Документирование политики информационной безопасности | | | Политика информационной безопасности должна быть руководством утверждена, издана и доведена до сведения всех сотрудников организации, а также сторонних организаций | |
| A.5.1.2 | Анализ политики информационной безопасности | | | Политика информационной безопасности организации должна быть подвергнута анализу и пересмотру через заданные промежутки времени или при появлении существенных изменений характеристик целей безопасности | |
| **А.6 Организация информационной безопасности** | | | | | |
| **А.6.1 Внутренняя организация**  Цель: Обеспечение управления информационной безопасностью в организации | | | | | |
| A.6.1.1 | | Обязанности руководства по обеспечению информационной безопасности | | Руководство организации должно постоянно поддерживать заданный уровень информационной безопасности путем внедрения системы менеджмента, а также путем распределения обязанностей и ответственности персонала за ее обеспечение | |
| A.6.1.2 | | Координация вопросов обеспечения информационной безопасности | | Действия по обеспечению информационной безопасности должны координироваться представителями различных подразделений организации, имеющими соответствующие функции и должностные обязанности | |
| A.6.1.3 | | Распределение обязанностей по обеспечению информационной безопасности | | Обязанности персонала по обеспечению информационной безопасности должны быть четко определены | |
| A.6.1.4 | | Процедура получения разрешения на использование средств обработки информации | | Руководство должно определить и внедрить процедуры получения разрешения на использование новых средств обработки информации | |
| A.6.1.5 | | Соглашения о соблюдении конфиденциальности | | Руководство организации должно определять условия конфиденциальности или вырабатывать соглашения о неразглашении информации в соответствии с целями защиты информации и регулярно их пересматривать | |
| A.6.1.6 | | Взаимодействие с компетентными органами | | Руководство организации должно поддерживать взаимодействие с соответствующими компетентными органами | |
| A.6.1.7 | | Взаимодействие с ассоциациями и профессиональными группами | | Руководство организации должно поддерживать соответствующее взаимодействие с профессиональными группами, ассоциациями и участвовать (организовывать) в конференциях (форумах) специалистов в области информационной безопасности | |
| A.6.1.8 | | Независимая проверка (аудит) информационной безопасности | | Порядок организации и управления информационной безопасностью и ее реализация (например, изменение целей и мер управления, политики, процессов и процедур обеспечения информационной безопасности) должны быть подвергнуты независимой проверке (аудиту) через определенные промежутки времени или при появлении существенных изменений в способах реализации мер безопасности | |
| **А.6.2 Обеспечение безопасности при наличии доступа сторонних организаций к информационным системам** | | | | | |
| Цель: Поддерживать безопасность информации и средств обработки информации организации при наличии доступа к ним сторонних организаций в процессах обработки и передачи этой информации | | | | | |
| A.6.2.1 | | Определение рисков, связанных со сторонними организациями | | | Перед предоставлением доступа сторонним организациям к информации и средствам ее обработки в процессе деятельности организации необходимо определять возможные риски для информации и средств ее обработки и реализовывать соответствующие им меры безопасности |
| A.6.2.2 | | Рассмотрение вопросов безопасности при работе с клиентами | | | Перед предоставлением клиентам права доступа к информации или активам организации необходимо определить и внедрить меры безопасности |
| A.6.2.3 | | Рассмотрение требований безопасности в соглашениях со сторонними организациями | | | Соглашения со сторонними организациями должны содержать все требования безопасности, включающие в себя правила доступа к процессам обработки, передачи информации или к управлению информацией или средствами обработки информации организации, а также и в случае приобретения дополнительных программных продуктов или организации сервисного обслуживания средств обработки информации |
| **А.7 Управление активами** | | | | | |
| **А.7.1 Ответственность за защиту активов организации** | | | | | |
| Цель: Обеспечивать соответствующую защиту активов организации | | | | | |
| A.7.1.1 | | Инвентаризация активов | | | Опись всех важных активов организации должна быть составлена и актуализирована |
| A.7.1.2 | | Владение активами | | | Вся информация и активы, связанные со средствами обработки информации, должны иметь назначенного во владение  представителя организации |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  Термин "владелец" (owner) определен как лицо или организация, на которую возложена установленная ответственность управления по контролю производства, разработке, поддержке, использованию и безопасности активов. Термин "владелец" не означает, что данное лицо фактически имеет права собственности на этот актив. | | | | | |
| A.7.1.3 | | Приемлемое использование активов | | | Правила безопасного использования информации и активов, связанных со средствами обработки информации, должны быть определены, документированы и реализованы |
| **А.7.2 Классификация информации** | | | | | |
| Цель: Обеспечить уверенность в том, что информация защищена на надлежащем уровне | | | | | |
| A.7.2.1 | | Основные принципы классификации | | | Информация должна быть классифицирована исходя из правовых требований, ее конфиденциальности, а также ценности и критичности для организации |
| A.7.2.2 | | Маркировка и обработка информации | | | В соответствии с принятой в организации системой классификации должна быть разработана и реализована совокупность процедур маркировки и обработки информации |
| **А.8 Правила безопасности, связанные с персоналом** | | | | | |
| **А.8.1 Перед трудоустройством**  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_   Под словом "трудоустройство" (employment) здесь поняты следующие ситуации: прием на работу (временную или постоянную), назначение на должность или перевод на другую должность, переоформление контрактов или аннулирование каких-либо из этих ситуаций.  Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и пользователи сторонней организации осознают свою ответственность и способны выполнять предусмотренные для них функции и снижать риск от воровства, мошенничества и нецелевого использования оборудования, а также от угроз безопасности информации | | | | | |
| A.8.1.1 | | Функции и обязанности персонала по обеспечению безопасности | | | Функции и обязанности персонала по обеспечению безопасности сотрудников, подрядчиков и пользователей сторонней организации должны быть определены и документированы в соответствии с требованиями информационной безопасности |
| A.8.1.2 | | Проверка при приеме на работу | | | Проверка всех кандидатов на постоянную работу, подрядчиков и пользователей сторонней организации должна быть проведена в соответствии с законами, инструкциями и правилами этики, с учетом требований бизнеса, характера информации, к которой будет осуществлен их доступ, и предполагаемых рисков |
| A.8.1.3 | | Условия трудового договора | | | Сотрудники, подрядчики и пользователи сторонней организации должны согласовать и подписать условия своего трудового договора, в котором установлены их ответственность и ответственность организации относительно информационной безопасности |
| **А.8.2 Работа по трудовому договору**  Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и пользователи сторонней организации осведомлены об угрозах и проблемах информационной безопасности, об их ответственности и обязательствах, ознакомлены с правилами и обучены процедурам для поддержания мер безопасности организации при выполнении ими своих служебных обязанностей и для снижения риска человеческого фактора для информационной безопасности | | | | | |
| A.8.2.1 | | Обязанности руководства | | | Руководство организации должно требовать, чтобы сотрудники, подрядчики и пользователи сторонней организации были ознакомлены с правилами и процедурами обеспечения мер безопасности в соответствии с установленными требованиями |
| A.8.2.2 | | Осведомленность, обучение и переподготовка в области информационной безопасности | | | Все сотрудники организации и, при необходимости, подрядчики и пользователи сторонних организаций должны проходить соответствующее обучение и переподготовку в целях регулярного получения информации о новых требованиях правил и процедур организации безопасности, необходимых для выполнения ими должностных функций |
| A.8.2.3 | | Дисциплинарная практика | | | К сотрудникам, совершившим нарушение требований безопасности, должна быть применена дисциплинарная практика, установленная в организации |
| **А.8.3 Увольнение или изменение трудового договора**  Цель: Обеспечить уверенность в том, что сотрудники, подрядчики и пользователи сторонней организации уведомлены об увольнении или изменении условий трудового договора в соответствии с установленным порядком | | | | | |
| A.8.3.1 | | Ответственность по окончании действия трудового договора | | | Ответственность по окончании действия трудового договора должна быть четко определена и установлена |
| A.8.3.2 | | Возврат активов | | | Сотрудники, подрядчики и пользователи сторонней организации обязаны вернуть все активы организации, находящиеся в их пользовании (владении), по истечении срока действия трудового договора или соглашения (увольнение) |
| A.8.3.3 | | Аннулирование прав доступа | | | Права доступа к информации и средствам обработки информации сотрудников, подрядчиков и пользователей сторонней организации должны быть аннулированы или уточнены по окончании действия трудового договора (увольнение) |
| **А.9 Физическая защита и защита от воздействия окружающей среды** | | | | | |
| **А.9.1 Охраняемые зоны**  Цель: Предотвращать несанкционированные физический доступ, повреждение и воздействия на помещения и информацию организации | | | | | |
| A.9.1.1 | | Периметр охраняемой зоны | | | Для защиты зон, где имеются информация и средства обработки информации, должны быть использованы периметры охраняемых зон (барьеры, такие как стены, проходные, оборудованные средствами контроля входа по идентификационным карточкам, или, где предусмотрен, контроль сотрудника регистрационной стойки) |
| A.9.1.2 | | Контроль доступа в охраняемую зону | | | Охраняемая зона должна быть защищена соответствующими средствами контроля входа, предполагающими обеспечить уверенность в том, что только авторизованный персонал может получить доступ в зону |
| A.9.1.3 | | Обеспечение безопасности зданий, производственных помещений и оборудования | | | Требования к обеспечению физической безопасности зданий, производственных помещений и оборудования должны быть разработаны и реализованы |
| A.9.1.4 | | Защита от внешних угроз и угроз со стороны окружающей среды | | | Требования к обеспечению физической защиты зданий, производственных помещений и оборудования от нанесения ущерба в результате пожара, наводнения, землетрясения, взрыва, общественных беспорядков и других природных и антропогенных факторов должны быть разработаны и реализованы |
| A.9.1.5 | | Выполнение работ в охраняемых зонах | | | Требования по физической защите и рекомендации по выполнению работ в охраняемых зонах должны быть разработаны и реализованы в инструкциях |
| A.9.1.6 | | Зоны общественного доступа, приема и отгрузки материальных ценностей | | | Места доступа, такие как зоны приема, отгрузки материальных ценностей и другие места, где неавторизованные лица могут проникнуть в помещения, должны быть под контролем и, по возможности, должны быть изолированы от средств обработки информации во избежание несанкционированного доступа |
| **А.9.2 Безопасность оборудования**  Цель: Предотвращать потерю, повреждение, хищение или компрометацию активов и прекращение деятельности организации | | | | | |
| A.9.2.1 | | Размещение и защита оборудования | | | Оборудование должно быть размещено и защищено так, чтобы уменьшить риски от воздействия окружающей среды и возможности несанкционированного доступа |
| A.9.2.2 | | Вспомогательные услуги | | | Оборудование необходимо защищать от перебоев в подаче электроэнергии и других сбоев, связанных с отказами в обеспечении вспомогательных услуг |
| A.9.2.3 | | Безопасность кабельной сети | | | Силовые и телекоммуникационные кабельные сети, по которым передаются данные или поддерживаются информационные услуги, необходимо защищать от перехвата информации или повреждения |
| A.9.2.4 | | Техническое обслуживание оборудования | | | Должно проводиться надлежащее регулярное техническое обслуживание оборудования для обеспечения его непрерывной работоспособности и сохранности |
| A.9.2.5 | | Обеспечение безопасности оборудования, используемого вне помещений организации | | | При обеспечении безопасности оборудования, используемого вне места его постоянной эксплуатации, должны быть учтены различные риски, связанные с работой вне помещений организации |
| A.9.2.6 | | Безопасная утилизация или повторное использование оборудования | | | Все компоненты оборудования, содержащие носители данных, должны быть проверены с целью удостовериться в том, что любые конфиденциальные данные и лицензионное программное обеспечение были удалены или скопированы безопасным образом до их утилизации (списания) |
| A.9.2.7 | | Вынос имущества с территории организации | | | Оборудование, информацию или программное обеспечение допускается выносить из помещения организации только на основании соответствующего разрешения |
| **А.10 Управление средствами коммуникаций и их функционированием** | | | | | |
| **А.10.1 Эксплуатация средств и ответственность**  Цель: Обеспечить надлежащее и безопасное функционирование средств обработки информации | | | | | |
| A.10.1.1 | | Документирование операционных процедур эксплуатации | | | Операционные процедуры должны документироваться, поддерживаться и быть доступными для всех авторизованных пользователей |
| A.10.1.2 | | Управление изменениями | | | Изменения в конфигурациях средств обработки информации и системах должны быть контролируемыми |
| A.10.1.3 | | Разграничение обязанностей | | | Обязанности и области ответственности должны быть разграничены в целях снижения возможностей несанкционированной или непреднамеренной модификации, или нецелевого использования активов организации |
| A.10.1.4 | | Разграничение средств разработки, тестирования и эксплуатации | | | Средства разработки, тестирования и эксплуатации должны быть разграничены в целях снижения риска несанкционированного доступа или изменения операционной системы |
| **А.10.2 Управление поставкой услуг лицами и/или сторонними организациями**  Цель: Реализовать и поддерживать требуемый уровень информационной безопасности и оказания услуг в соответствии с договорами об оказании услуг сторонними организациями (внешними лицами и/или организациями) | | | | | |
| A.10.2.1 | | Оказание услуг | | | Должна быть обеспечена уверенность в том, что меры управления информационной безопасностью, включенные в договор об оказании услуг сторонней организации, реализованы, функционируют и поддерживаются сторонней организацией |
| A.10.2.2 | | Мониторинг и анализ услуг, оказываемых сторонними лицами и/или организациями | | | Необходимо регулярно проводить мониторинг, аудит и анализ услуг, отчетов и актов, обеспечиваемых сторонней организацией |
| A.10.2.3 | | Изменения при оказании сторонними организациями услуг по обеспечению безопасности | | | Изменения при оказании услуг по обеспечению безопасности, включая внедрение и совершенствование существующих требований, процедур и мер обеспечения информационной безопасности, должны быть управляемыми с учетом оценки критичности систем и процессов бизнеса, а также результатов переоценки рисков |
| **А.10.3 Планирование производительности и загрузки систем**  Цель: Свести к минимуму риск сбоев в работе систем | | | | | |
| A.10.3.1 | | Управление производительностью | | | Необходимо осуществлять прогнозирование, мониторинг и корректировку потребности мощности системы для обеспечения требуемой ее производительности |
| A.10.3.2 | | Приемка систем | | | Должны быть определены критерии принятия новых и модернизированных информационных систем, новых версий программного обеспечения, а также проведено тестирование систем в процессе их разработки и приемки |
| **А.10.4 Защита от вредоносного кода и мобильного кода**  Цель: Защищать целостность программного обеспечения и массивов информации | | | | | |
| A.10.4.1 | | Меры защиты от вредоносного кода | | | Должны быть реализованы меры по обнаружению, предотвращению проникновения и восстановлению после проникновения вредоносного кода, а также должны быть установлены процедуры обеспечения соответствующего оповещения пользователей |
| A.10.4.2 | | Меры защиты от мобильного кода | | | Там, где разрешено использование мобильного кода, конфигурация системы должна обеспечивать уверенность в том, что авторизованный мобильный код функционирует в соответствии с четко определенной политикой безопасности, а исполнение операции с использованием неавторизованного мобильного кода будет предотвращено |
| **А.10.5 Резервирование**  Цель: Поддерживать целостность и доступность информации и средств обработки информации | | | | | |
| A.10.5.1 | | Резервирование информации | | | Резервные копии информации и программного обеспечения должны создаваться, проверяться и тестироваться на регулярной основе в соответствии с принятыми требованиями резервирования |
| **А.10.6 Управление безопасностью сети**  Цель: Обеспечить защиту информации в сетях и защиту поддерживающей инфраструктуры | | | | | |
| A.10.6.1 | | Средства контроля сети | | | Сети должны быть адекватно управляемыми и контролируемыми в целях защиты от угроз и поддержания безопасности систем и приложений, использующих сеть, включая информацию, передаваемую по сетям |
| A.10.6.2 | | Безопасность сетевых сервисов | | | Меры обеспечения безопасности, уровни обслуживания для всех сетевых услуг и требования управления должны быть определены и включены в любой договор о сетевых услугах независимо от того, предоставляются ли эти услуги своими силами или сторонней организацией |
| **А.10.7 Обращение с носителями информации**  Цель: Предотвратить несанкционированное разглашение, модификацию, удаление или уничтожение активов и прерывание бизнес-процессов | | | | | |
| A.10.7.1 | | Управление съемными носителями информации | | | Для управления съемными носителями информации должны существовать соответствующие процедуры |
| A.10.7.2 | | Утилизация носителей информации | | | Носители информации, когда в них больше нет необходимости, должны быть надежно и безопасно утилизированы с помощью формализованных процедур |
| A.10.7.3 | | Процедуры обработки информации | | | Для обеспечения защиты информации от несанкционированного раскрытия или неправильного использования необходимо установить процедуры обработки и хранения информации |
| A.10.7.4 | | Безопасность системной документации | | | Системная документация должна быть защищена от несанкционированного доступа |
| **А.10.8 Обмен информацией**  Цель: Поддерживать безопасность информации и программного обеспечения при обмене внутри организации и со сторонними организациями | | | | | |
| A.10.8.1 | | Политики и процедуры обмена информацией | | | Должны существовать формализованные процедуры, требования и меры контроля, обеспечивающие защиту обмена информацией при использовании связи всех типов |
| A.10.8.2 | | Соглашения по обмену информацией | | | Между организацией и сторонними организациями должны быть заключены соглашения по обмену информацией и программным обеспечением |
| A.10.8.3 | | Защита физических носителей информации при транспортировке | | | Носители информации должны быть защищены от несанкционированного доступа, неправильного использования или повреждения во время их транспортировки за пределами территории организации |
| A.10.8.4 | | Электронный обмен сообщениями | | | Информация, используемая в электронном обмене сообщениями, должна быть защищена надлежащим образом |
| A.10.8.5 | | Системы бизнес-информации | | | Требования и процедуры должны быть разработаны и внедрены для защиты информации, связанной с взаимодействием систем бизнес-информации |
| **А.10.9 Услуги электронной торговли**  Цель: Обеспечить безопасность услуг электронной торговли и их безопасное использование | | | | | |
| A.10.9.1 | | Электронная торговля | | | Информация, используемая в электронной торговле, проходящая по общедоступным сетям, должна быть защищена от мошенничества, оспаривания контрактов, а также от несанкционированного разглашения и модификации |
| A.10.9.2 | | Трансакции в режиме реального времени (on-line) | | | Информация, используемая в трансакциях в режиме реального времени (on-line), должна быть защищена для предотвращения неполной передачи, неправильной маршрутизации, несанкционированного изменения сообщений, несанкционированного разглашения, несанкционированного копирования или повторного воспроизведения сообщений |
| A.10.9.3 | | Общедоступная информация | | | Информация, предоставляемая через общедоступную систему, должна быть защищена от несанкционированной модификации |
| **А.10.10 Мониторинг**  Цель: Обнаруживать несанкционированные действия, связанные с обработкой информации | | | | | |
| A.10.10.1 | | Ведение журналов аудита | | | Должны быть обеспечены ведение и хранение в течение определенного периода времени журналов аудита, регистрирующих действия пользователей, нештатные ситуации и события информационной безопасности, в целях помощи в будущих расследованиях и проведении мониторинга контроля доступа |
| A.10.10.2 | | Мониторинг использования средств обработки информации | | | Должны быть установлены процедуры, позволяющие вести мониторинг и регулярный анализ результатов мониторинга использования средств обработки информации |
| A.10.10.3 | | Защита информации журналов регистрации | | | Средства регистрации и информация журналов регистрации должны быть защищены от вмешательства и несанкционированного доступа |
| A.10.10.4 | | Журналы регистрации действий администратора и оператора | | | Действия системного администратора и системного оператора должны быть регистрируемыми |
| A.10.10.5 | | Регистрация неисправностей | | | Неисправности должны быть зарегистрированы, проанализированы и устранены |
| A.10.10.6 | | Синхронизация часов | | | Часы всех соответствующих систем обработки информации в пределах организации или охраняемой зоны должны быть синхронизированы с помощью единого источника точного времени |
| **А.11 Контроль доступа** | | | | | |
| **А.11.1 Бизнес-требования к контролю доступа**  Цель: Контролировать доступ к информации | | | | | |
| A.11.1.1 | | Политика контроля доступа | | | Политика контроля доступа должна быть установлена и документирована с учетом потребностей бизнеса и безопасности информации |
| **А.11.2 Управление доступом пользователей**  Цель: Предотвратить несанкционированный доступ пользователей к информационным системам и обеспечить авторизованный доступ пользователей к этим системам | | | | | |
| A.11.2.1 | | Регистрация пользователей | | | Должна быть установлена формализованная процедура регистрации и снятия с регистрации пользователей для предоставления и отмены доступа ко всем информационным системам и услугам |
| A.11.2.2 | | Управление привилегиями | | | Предоставление и использование привилегий должно быть ограниченным и контролируемым |
| A.11.2.3 | | Управление паролями пользователей | | | Предоставление паролей должно быть контролируемым посредством формализованного процесса управления |
| A.11.2.4 | | Пересмотр прав доступа пользователей | | | Руководство должно периодически осуществлять пересмотр прав доступа пользователей, используя формализованный процесс |
| **А.11.3 Ответственность пользователей**  Цель: Предотвращать несанкционированный доступ пользователей, а также компрометацию или кражу информации и средств обработки информации | | | | | |
| A.11.3.1 | | Использование паролей | | | Пользователи должны соблюдать правила безопасности при выборе и использовании паролей |
| A.11.3.2 | | Оборудование, оставленное пользователем без присмотра | | | Пользователи должны обеспечивать соответствующую защиту оборудования, оставленного без присмотра |
| A.11.3.3 | | Правила "чистого стола" и "чистого экрана" | | | Должны быть приняты правила "чистого стола" для документов на бумажных носителях и сменных носителей данных, а также правила "чистого экрана" для средств обработки информации |
| **А.11.4 Контроль сетевого доступа**  Цель: Предотвратить несанкционированный доступ к сетевым сервисам | | | | | |
| A.11.4.1 | | Политика в отношении использования сетевых услуг | | | Пользователям следует предоставлять доступ только к тем услугам, по отношению к которым они специально были авторизованы |
| A.11.4.2 | | Аутентификация пользователей для внешних соединений | | | Для контроля доступа удаленных пользователей должны быть применены соответствующие методы аутентификации |
| A.11.4.3 | | Идентификация оборудования в сетях | | | Автоматическая идентификация оборудования должна рассматриваться как средство аутентификации соединений, осуществляемых с определенных мест и с определенным оборудованием |
| A.11.4.4 | | Защита диагностических и конфигурационных портов при удаленном доступе | | | Физический и логический доступ к портам конфигурации и диагностики должен быть контролируемым |
| A.11.4.5 | | Принцип разделения в сетях | | | В сетях должны быть применены принципы разделения групп информационных услуг, пользователей и информационных систем |
| A.11.4.6 | | Контроль сетевых соединений | | | Подключение пользователей к совместно используемым сетям, особенно к тем, которые выходят за территорию организации, необходимо ограничивать в соответствии с политикой контроля доступа и требованиями бизнес-приложений (см. А.11.1) |
| A.11.4.7 | | Контроль маршрутизации в сети | | | Должны быть внедрены средства управления и контроля маршрутизации в сети с целью исключить нарушения правил контроля доступа для бизнес-приложений, вызываемые соединениями и потоками информации |
| **А.11.5 Контроль доступа к операционной системе**  Цель: Предотвратить несанкционированный доступ к операционным системам | | | | | |
| A.11.5.1 | | Безопасные процедуры регистрации | | | Контроль доступа к операционным системам должен быть обеспечен безопасной процедурой регистрации |
| A.11.5.2 | | Идентификация и аутентификация пользователя | | | Все пользователи должны иметь уникальные идентификаторы (ID) только для персонального использования, а для подтверждения заявленной личности пользователя должны быть выбраны подходящие методы аутентификации |
| A.11.5.3 | | Система управления паролями | | | Системы управления паролями должны быть интерактивными и обеспечивать высокое качество паролей |
| A.11.5.4 | | Использование системных утилит | | | Использование системных утилит, которые могут преодолеть средства контроля операционных систем и приложений, необходимо ограничивать и строго контролировать |
| A.11.5.5 | | Периоды бездействия в сеансах связи | | | Необходимо обеспечить завершение сеансов связи после определенного периода бездействия |
| A.11.5.6 | | Ограничение времени соединения | | | Ограничение времени соединения должно быть использовано для обеспечения дополнительной безопасности |
| **А.11.6 Контроль доступа к прикладным системам и информации**  Цель: Предотвратить несанкционированный доступ к прикладным системам и информации | | | | | |
| A.11.6.1 | | Ограничения доступа к информации | | | Доступ к информации и функциям прикладных систем пользователей и обслуживающего персонала должен быть предоставлен только в соответствии с определенными политиками контроля доступа |
| A.11.6.2 | | Изоляция систем, обрабатывающих важную информацию | | | Системы, обрабатывающие важную информацию, должны иметь выделенную (изолированную) вычислительную среду |
| **А.11.7 Работа с переносными устройствами и работа в дистанционном режиме**  Цель: Обеспечить информационную безопасность при использовании переносных устройств и средств, необходимых для работы в дистанционном режиме | | | | | |
| A.11.7.1 | | Работа с переносными устройствами | | | Необходимо иметь в наличии формализованную политику для защиты от рисков при использовании переносных устройств |
| A.11.7.2 | | Работа в дистанционном режиме | | | Для работы в дистанционном режиме необходимо разработать и реализовать политику, оперативные планы и процедуры |
| **А.12 Разработка, внедрение и обслуживание информационных систем** | | | | | |
| **А.12.1 Требования к безопасности информационных систем**  Цель: Обеспечить уверенность в том, что безопасность является неотъемлемым свойством внедряемых информационных систем, и обеспечить выполнение требований безопасности при разработке и эксплуатации систем | | | | | |
| A.12.1.1 | | Анализ и детализация требований безопасности | | | В формулировках требований бизнеса для новых информационных систем или совершенствования существующих должны быть детализированы требования безопасности |
| **А.12.2 Правильная обработка данных в приложениях**  Цель: Предотвратить ошибки, потерю, несанкционированную модификацию или неправильное использование информации в приложениях | | | | | |
| A.12.2.1 | | Проверка достоверности входных данных | | | Входные данные для приложений должны быть подвергнуты процедуре подтверждения с целью установления их достоверности |
| A.12.2.2 | | Контроль обработки данных в приложениях | | | Для обнаружения искажений (ошибок или преднамеренных действий) при обработке информации в требования к функциям приложений должны быть включены требования по выполнению контрольных проверок |
| A.12.2.3 | | Целостность сообщений | | | Должны быть определены требования для обеспечения аутентичности и защиты целостности сообщений в приложениях, а также реализованы соответствующие средства контроля |
| A.12.2.4 | | Подтверждение достоверности выходных данных | | | Данные, выводимые из приложения, необходимо подвергать проверке на корректность, чтобы обеспечить уверенность в том, что обработка информации выполнена правильно |
| **А.12.3 Криптографические средства защиты**  Цель: Защищать конфиденциальность, аутентичность или целостность информации криптографическими средствами | | | | | |
| A.12.3.1 | | Политика использования криптографических средств защиты | | | Должны быть разработаны и внедрены правила использования криптографических средств защиты информации |
| A.12.3.2 | | Управление ключами | | | Для реализации организацией криптографических методов защиты должна быть использована система управления ключами |
| **А.12.4 Безопасность системных файлов**  Цель: Обеспечить безопасность системных файлов | | | | | |
| A.12.4.1 | | Контроль программного обеспечения, находящегося в промышленной эксплуатации | | | Необходимо обеспечить контроль за процессом внедрения программного обеспечения в промышленную эксплуатацию |
| A.12.4.2 | | Защита данных тестирования системы | | | Данные тестирования следует тщательно отбирать, защищать и контролировать |
| A.12.4.3 | | Контроль доступа к исходным кодам | | | Доступ к исходным кодам должен быть ограничен |
| **А.12.5 Безопасность в процессах разработки и поддержки**  Цель: Поддерживать безопасность программного обеспечения прикладных систем и содержащейся в них информации | | | | | |
| A.12.5.1 | | Процедуры контроля изменений | | | Внесение изменений должно быть проверено с использованием соответствующих формализованных процедур контроля изменений |
| A.12.5.2 | | Технический анализ прикладных систем после внесения изменений в операционные системы | | | При внесении изменений в операционные системы необходимо провести анализ и тестирование критичных бизнес-приложений с целью удостовериться в отсутствии негативного влияния на работу и безопасность организации |
| A.12.5.3 | | Ограничения на внесение изменений в пакеты программ | | | Необходимо избегать модификаций пакетов программ, а все требуемые изменения должны подлежать строгому контролю |
| A.12.5.4 | | Утечка информации | | | Возможности для утечки информации должны быть предотвращены |
| A.12.5.5 | | Разработка программного обеспечения с привлечением сторонних организаций | | | Разработка программного обеспечения с привлечением сторонних организаций должна проводиться под контролем и при мониторинге организации |
| **А.12.6 Менеджмент технических уязвимостей**  Цель: Снизить риски, являющиеся результатом использования опубликованных технических уязвимостей | | | | | |
| A.12.6.1 | | Управление техническими уязвимостями | | | Необходимо получать своевременную информацию о технических уязвимостях используемых информационных систем, оценивать опасность таких уязвимостей и принимать соответствующие меры по устранению связанного с ними риска |
| **А.13 Управление инцидентами информационной безопасности** | | | | | |
| **А.13.1 Оповещение о нарушениях и недостатках информационной безопасности**  Цель: Обеспечить оперативность оповещения о событиях информационной безопасности и нарушениях, связанных с информационными системами, а также своевременность корректирующих действий | | | | | |
| A.13.1.1 | | | Оповещение о случаях нарушения информационной безопасности | | О случаях нарушения информационной безопасности следует сообщать по соответствующим каналам управления незамедлительно, насколько это возможно |
| A.13.1.2 | | | Оповещение о недостатках безопасности | | Все сотрудники, подрядчики и пользователи сторонних организаций, пользующиеся информационными системами и услугами, должны незамедлительно сообщать о любых замеченных или предполагаемых нарушениях безопасности в системах или услугах |
| **А.13.2 Управление инцидентами информационной безопасности и его усовершенствование**  Цель: Обеспечить последовательный и эффективный подход к управлению инцидентами информационной безопасности | | | | | |
| A.13.2.1 | | | Ответственность и процедуры | | Должны быть установлены ответственность руководства и процедуры, позволяющие обеспечить быстрое, эффективное и последовательное реагирование на инциденты информационной безопасности |
| A.13.2.2 | | | Извлечение уроков из инцидентов информационной безопасности | | Должны быть определены механизмы, позволяющие вести мониторинг и регистрацию инцидентов информационной безопасности по типам, объемам и стоимостям |
| A.13.2.3 | | | Сбор доказательств | | На случай, если инцидент информационной безопасности может привести к судебному разбирательству (гражданскому или уголовному) против лица или организации, информация должна быть собрана, сохранена и представлена согласно правилам оформления доказательств, изложенным в соответствующих документах |
| **А.14 Управление непрерывностью бизнеса** | | | | | |
| **А.14.1 Вопросы информационной безопасности управления непрерывностью бизнеса**  Цель: На случай, если инцидент информационной безопасности может привести к судебному разбирательству (гражданскому или уголовному) против лица или организации, информация должна быть собрана, сохранена и представлена согласно правилам оформления доказательств, изложенным в соответствующих документах | | | | | |
| A.14.1.1 | | | Включение информационной безопасности в процесс управления непрерывностью бизнеса | | Должен быть разработан и поддержан управляемый процесс обеспечения непрерывности бизнеса во всей организации с учетом требований информационной безопасности, необходимых для обеспечения непрерывности бизнеса организации |
| A.14.1.2 | | | Непрерывность бизнеса и оценка риска | | События, которые могут стать причиной прерывания бизнес-процессов, должны быть связаны с оценками вероятности и степени воздействия таких прерываний, а также с их последствиями для информационной безопасности |
| A.14.1.3 | | | Разработка и внедрение планов непрерывности бизнеса, включающих в себя информационную безопасность | | Должны быть разработаны и внедрены планы для поддержки или восстановления работы и обеспечения доступности информации на требуемом уровне и в требуемые сроки после прерывания или отказа критических бизнес-процессов |
| A.14.1.4 | | | Структура плана обеспечения непрерывности бизнеса | | Должна быть создана единая структура планов непрерывности бизнеса, позволяющая обеспечить непротиворечивость всех планов для последовательного выполнения всех требований к информационной безопасности и для расстановки приоритетов при тестировании и обслуживании |
| A.14.1.5 | | | Тестирование, поддержка и пересмотр планов по обеспечению непрерывности бизнеса | | Планы по обеспечению непрерывности бизнеса должны подлежать регулярному пересмотру и обновлению с целью обеспечить их актуальность и эффективность |
| **А.15 Соответствие требованиям** | | | | | |
| **А.15.1 Соответствие правовым требованиям**  Цель: Предотвращать любые нарушения норм уголовного и гражданского права, требований, установленных нормативно-правовыми актами, регулирующими органами или договорными обязательствами, а также требований безопасности | | | | | |
| A.15.1.1 | | | Определение применимых норм | | Все применимые нормы, установленные законодательством и исполнительными органами власти, требования договорных обязательств и порядок их выполнения следует четко определить, документировать и поддерживать на актуальном уровне для каждой информационной системы и организации |
| A.15.1.2 | | | Права на интеллектуальную собственность | | Должны быть внедрены соответствующие процедуры для применения законодательных, регулирующих и контрактных требований к используемым материалам с учетом прав на интеллектуальную собственность, а также прав на использование программных продуктов, являющихся предметом частной собственности |
| A.15.1.3 | | | Защита учетных записей организации | | Важные учетные записи организации должны быть защищены от утраты, разрушения и фальсификации в соответствии с требованиями, установленными законами, документами органов исполнительной власти, контрактами и требованиями бизнеса |
| A.15.1.4 | | | Защита данных и конфиденциальность персональной информации | | Защита данных и конфиденциальность персональной информации должны быть обеспечены в соответствии с требованиями законов, нормативных актов и, где это применимо, в соответствии с положениями контрактов |
| A.15.1.5 | | | Предотвращение нецелевого использования средств обработки информации | | Должны быть применены меры контроля для предотвращения нецелевого использования средств обработки информации |
| A.15.1.6 | | | Регулирование использования средств криптографической защиты | | Средства криптографической защиты должны быть использованы в соответствии с законами, нормативными актами и соответствующими соглашениями |
| **А.15.2 Соответствие политикам и стандартам безопасности и техническое соответствие требованиям безопасности**  Цель: Обеспечить соответствие систем организационным политикам и стандартам безопасности | | | | | |
| A.15.2.1 | | | Соответствие политикам и стандартам безопасности | | Руководители должны обеспечить, чтобы все процедуры безопасности в их сфере ответственности были выполнены правильно и соответствовали политикам и стандартам безопасности |
| A.15.2.2 | | | Проверка технического соответствия требованиям безопасности | | Информационные системы следует регулярно проверять на соответствие требованиям стандартов безопасности |
| **А.15.3 Вопросы аудита информационных систем**  Цель: Повышение эффективности процесса аудита информационных систем и снижение негативного влияния, связанного с данным процессом | | | | | |
| A.15.3.1 | | | Меры управления аудитом информационных систем | | Требования и процедуры аудита, включающие в себя проверки операционных систем, необходимо тщательно планировать и согласовывать, чтобы свести к минимуму риск прерывания бизнес-процессов |
| A.15.3.2 | | | Защита инструментальных средств аудита информационных систем | | Доступ к инструментальным средствам аудита информационных систем необходимо защищать для предотвращения любой возможности их неправильного использования или компрометации |

ПРОЦЕССЫ

|  |  |
| --- | --- |
| Принцип ОЭСР | Соответствующий процесс СМИБ и стадия PDCA |
| **Осведомленность**  Участники должны быть осведомлены о необходимости обеспечения безопасности информационных систем и сетей и о том, что они могут сделать для повышения уровня безопасности | Данные мероприятия являются частью стадии "Осуществление" (см. 4.2.2 и 5.2) |
| **Ответственность**  Все участники являются ответственными за безопасность информационных систем и сетей | Данные мероприятия являются частью стадии "Осуществление" (см. 4.2.2 и 5.1) |
| **Реагирование**  Участники должны действовать совместно и своевременно, чтобы предотвращать, обнаруживать инциденты безопасности и реагировать на них | Является частью стадии "Проверка" деятельности по мониторингу (см. 4.2.3, раздел 6 и 7.3) и мероприятий по реагированию стадии "Действие" (см. 4.2.4, 8.1, 8.2 и 8.3). Данные мероприятия могут быть также охвачены некоторыми элементами стадий "Планирование" и "Проверка" |
| **Оценка риска**  Участники должны проводить оценку рисков | Этот вид деятельности является частью стадии "Планирование" (см. 4.2.1), а повторная оценка (переоценка) риска является частью стадии "Проверка" (см. 4.2.3, раздел 6 и 7.3) |
| **Разработка и внедрение безопасности**  Участники должны внедрить безопасность как важный элемент информационных систем и сетей | После выполнения оценки рисков выбирают меры управления для обработки рисков как часть стадии "Планирование" (см. 4.2.1). Стадия "Осуществление" (см. 4.2.2 и 5.2) охватывает затем внедрение и обеспечение функционирования этих мер управления |
| **Менеджмент безопасности**  Участники должны применять всесторонний подход к менеджменту безопасности | Менеджмент рисков представляет собой процесс, включающий в себя предотвращение, обнаружение инцидентов и реагирование на них, сопровождение, анализ и аудит. Все эти вопросы решают на стадиях "Планирование", "Осуществление", "Проверка" и "Действие" |
| **Повторная оценка**  Участники должны анализировать и повторно оценивать состояние безопасности информационных систем и сетей, и вносить соответствующие изменения в политику, практику, меры и процедуры безопасности | Переоценка (повторная оценка) информационной безопасности является частью стадии "Проверка" (см. 4.2.3, раздел 6 и 7.3), на которой должны быть предприняты регулярные анализы эффективности системы менеджмента информационной безопасности, а повышение уровня безопасности является частью стадии "Действие" (см. 4.2.4, 8.1, 8.2 и 8.3) |

СТАНДАРТЫ

|  |  |  |
| --- | --- | --- |
| Настоящий стандарт | ИСО 9001:2000 | ИСО 14001:2004 |
| Введение | Введение | Введение |
| Общие положения | Общие положения |  |
| Процессный подход | Процессный подход |  |
|  | Связь с ИСО 9004 [9] |  |
| Возможность совместного использования с другими системами управления | Совместимость с другими системами менеджмента |  |
| 1 Область применения | 1 Область применения | 1 Область применения |
| 1.1 Общие положения | 1.1 Общие положения |  |
| 1.2 Применение | 1.2 Применение |  |
| 2 Нормативные ссылки | 2 Нормативные ссылки | 2 Нормативные ссылки |
| 3 Термины и определения | 3 Термины и определения | 3 Термины и определения |
| 4 Система менеджмента информационной безопасности | 4 Система менеджмента качества | 4 Требования системы управления в области охраны окружающей среды |
| 4.1 Общие требования | 4.1 Общие требования | 4.1 Общие требования |
| 4.2 Разработка СМИБ. Управление СМИБ |  |  |
| 4.2.1 Разработка СМИБ |  |  |
| 4.2.2 Внедрение и функционирование СМИБ |  | 4.4 Внедрение и эксплуатация |
| 4.2.3 Проведение мониторинга и анализа СМИБ | 8.2.3 Мониторинг и измерение процессов | 4.5.1 Мониторинг и измерение |
|  | 8.2.4 Мониторинг и измерение продукции |  |
| 4.2.4 Поддержка и улучшение СМИБ | - | - |
| 4.3 Требования к документации | 4.2 Требования к документации |  |
| 4.3.1 Общие положения | 4.2.1 Общие положения  4.2.2 Руководство по качеству | - |
| 4.3.2 Управление документами | 4.3.2 Управление документацией | 4.4.5 Меры контроля документации |
| 4.3.3 Управление записями | 4.2.4 Управление записями | 4.5.4 Меры контроля в отношении учетных записей |
| 5 Ответственность руководства | 5 Ответственность руководства |  |
| 5.1 Обязательства руководства | 5.1 Обязательства руководства |  |
|  | 5.2 Ориентация на потребителя |  |
|  | 5.3 Политика в области качества | 4.2 Политика в области охраны окружающей среды |
|  | 5.4 Планирование | 4.3 Планирование |
|  | 5.5 Ответственность, полномочия и обмен информацией |  |
| 5.2 Управление ресурсами | 6 Управление ресурсами |  |
| 5.2.1 Обеспечение ресурсами | 6.1 Обеспечение ресурсами  6.2 Человеческие ресурсы |  |
| 5.2.2 Подготовка, осведомленность и квалификация персонала | 6.2.2 Компетентность, осведомленность и подготовка  6.3 Инфраструктура  6.4 Производственная среда | 4.4.2 Обучение, осведомленность и компетентность |
| 6 Внутренние аудиты СМИБ | 8.2.2 Внутренние аудиты (проверки) | 4.5.5 Внутренний аудит |
| 7 Анализ СМИБ со стороны руководства | 5.6 Анализ со стороны руководства | 4.6 Контрольный анализ со стороны руководства |
| 7.1 Общие положения | 5.6.1 Общие положения |  |
| 7.2 Входные данные для анализа СМИБ | 5.6.2 Входные данные для проведения контрольного анализа |  |
| 7.3 Выходные данные анализа СМИБ | 5.6.3 Выходные данные контрольного анализа |  |
| 8 Улучшение СМИБ | 8.5 Совершенствование |  |
| 8.1 Постоянное улучшение | 8.5.2 Непрерывное совершенствование |  |
| 8.2 Корректирующие действия | 8.5.3 Корректирующие действия | 4.5.3 Несоответствие, коррективные и превентивные действия |
| 8.3 Предупреждающие действия | 8.5.4 Превентивные действия |  |
| Приложение А Цели и меры управления | - | Приложение А Руководство по использованию этого стандарта |
| Приложение В Принципы ОЭСР и настоящий стандарт | - | - |
| Приложение С Сравнение структуры настоящего стандарта со структурами международных стандартов ИСО 9001:2000, ИСО 14001:2004 | Приложение А Соответствие ИСО 9001:2000 и ИСО 14001:2004 | Соответствие между ИСО 14001:2004 и ИСО 9001:2000 |
| Приложение D Сведения о соответствии национальных стандартов Российской Федерации ссылочным международным стандартам | - |  |

ЗАКЛЮЧЕНИЕ

Данный стандарт прежде всего адресован крупным или особо важным организациям, обеспечение информационной безопасности которых критично для безопасности.

Также большое внимание уделяется возможным действиям по устранению рисков и контролю. Видно, что документ был написан на широкие массы с должным подходом и профессионализмом. На высоком уровне абстракции такие активности ИБ вполне реализуемы.

Судя по всему в дальнейшем Фреймворк будет активно расширяться и включит в себя ещё много других высокоуровневых функций ИБ.

В целом получается ещё одна важная часть в процессе управления рисками ИБ, грамотное применение которой будет зависеть также и от того, в каком виде он будет окончательно закреплён в определённой компании.