ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ БЕЛАРУСЬ

СТБ ISO/ПР1 28000

Безопасность и устойчивость
СИСТЕМЫ МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ
Требования

Бяспека і стабільнасць
СІСТЭМЫ МЕНЕДЖМЕНТУ БЯСПЕКІ
Патрабаванні

(ISO 28000:2022, IDT)

Настоящий проект стандарта
не подлежит применению до его утверждения

Госстандарт
Минск

УДК МКС 03.100.01; 03.100.70

Ключевые слова: безопасность, система менеджмента безопасности, контекст организации, лидерство, планирование, поддержка, операционная деятельность, оценивание пригодности, улучшение

Предисловие

Цели, основные принципы, положения по государственному регулированию и управлению в области технического нормирования и стандартизации установлены Законом Республики Беларусь «О техническом нормировании и стандартизации».

1 ПОДГОТОВЛЕН научно-производственным республиканским унитарным предприятием «Белорусский государственный институт стандартизации и сертификации» (БелГИСС) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 3

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Государственного комитета по стандартизации Республики Беларусь от ___ _____ 20___ г. № ___

3 Настоящий стандарт идентичен международному стандарту ISO 28000:2022 «Безопасность и устойчивость. Системы менеджмента безопасности. Требования» («Security and resilience – Security management systems – Requirements», IDT).

Международный стандарт разработан техническим комитетом по стандартизации ISO/TC 292 «Безопасность и устойчивость» Международной организации по стандартизации (ISO).

4 ВВЕДЕН ВПЕРВЫЕ

Издан на русском языке

Содержание

Введение

Большинство организаций сталкиваются с растущей неопределенностью и неустойчивостью среды безопасности. Как следствие, они сталкиваются с проблемами безопасности, воздействующими на их цели, которые они хотят решать систематически в рамках своей системы менеджмента. Формальный подход к менеджменту безопасности может непосредственно влиять на деловые возможности и авторитет организации.

Настоящий стандарт устанавливает требования к системе менеджмента безопасности, включая те аспекты, которые имеют решающее значение для обеспечения безопасности цепи поставок. Он требует от организации:

- оценивать среду безопасности, в которой она работает, включая цепь поставок (в том числе зависимости и взаимозависимости);
- определить, приняты ли адекватные меры безопасности для результативного менеджмента рисков, связанных с безопасностью;
- осуществлять менеджмент соблюдений законодательных, нормативных и добровольных обязательств, к которым присоединяется организация;
- согласовывать процессы и средства управления безопасности, включая соответствующие восходящие и нисходящие процессы и средства управления цепи поставок, для достижения целей организации.

Менеджмент безопасности связан со многими аспектами менеджмента бизнеса. Он включает в себя все виды деятельности, управляемые организациями или находящиеся под их влиянием, включая, но не ограничиваясь теми, которые влияют на цепь поставок. Следует рассматривать все виды деятельности, функции и операции, которые воздействуют на менеджмент безопасности организации, включая (но не ограничиваясь) ее цепь поставок.

Что касается цепи поставок, необходимо учитывать, что цепи поставок динамичны по своей природе. Поэтому некоторые организации, управляющие несколькими цепями поставок, могут требовать от своих поставщиков соблюдения соответствующих стандартов безопасности в качестве условия включения в эту цепь поставок для выполнения требований по менеджменту безопасности.

В настоящем стандарте применяется модель Планируй – Делай – Проверяй – Действуй (PDCA) для планирования, создания, внедрения, эксплуатации, мониторинга, анализа, поддержания и постоянного улучшения результативности системы менеджмента безопасности организации, см. таблицу 1 и рисунок 1.

Таблица 1 – Объяснение модели PDCA

Планируй (Устанавливай)	Установить политику, цели, задачи, средства управления в области безопасности, процессы и процедуры, относящиеся к улучшению безопасности, для достижения результатов, которые соответствуют общей политике и целям организации
Делай (Внедряй и действуй)	Внедрить и использовать политику, средства управления, процессы и процедуры в области безопасности
Проверяй (Осуществляй мониторинг и анализ)	Осуществить мониторинг и анализ пригодности в соответствии с политикой и целями в области безопасности, представление результатов руководству для анализа, а также определение и согласование действий по исправлению и улучшению ситуации
Действуй (Поддерживай и улучшай)	Поддерживать и улучшать систему менеджмента безопасности путем принятия корректирующих действий на основе результатов анализа со стороны руководства и повторной оценки области применения системы менеджмента безопасности, а также политики и целей в области безопасности

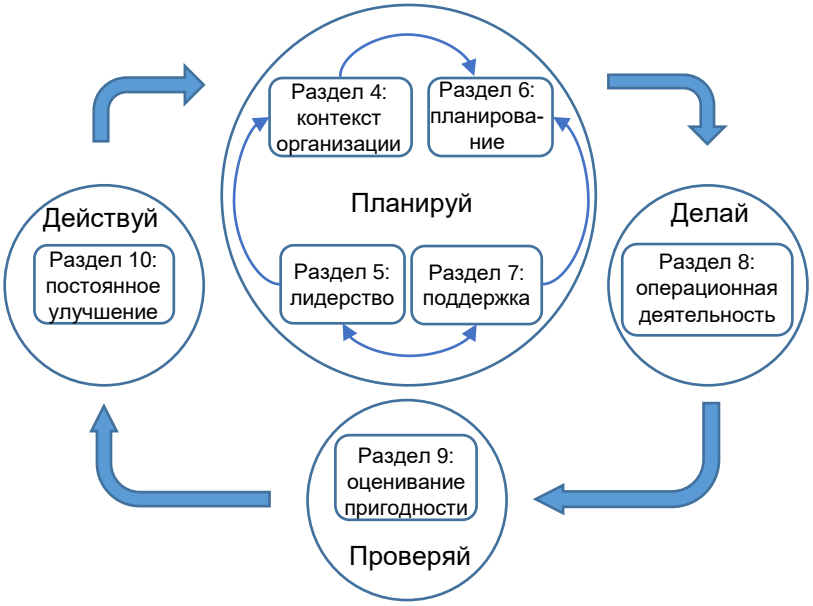


Рисунок 1 – Модель PDCA, применяемая к системе менеджмента безопасности

Это обеспечивает определенную степень согласованности с другими стандартами на системы менеджмента, такими как ISO 9001, ISO 14001, ISO 22301, ISO/IEC 27001, ISO 45001 и т.д., тем самым поддерживая последовательное и интегрированное внедрение и функционирование с соответствующими системами менеджмента.

Для организаций, которые этого пожелают, соответствие системы менеджмента безопасности настоящему стандарту может быть верифицировано в процессе внешнего или внутреннего аудита.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ БЕЛАРУСЬ

Безопасность и устойчивость СИСТЕМЫ МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ Требования

Бяспека і стабільнасць СІСТЭМЫ МЕНЕДЖМЕНТУ БЯСПЕКІ Патрабаванні

Security and resilience
Security management systems
Requirements

Дата введения _____

1 Область применения

Настоящий стандарт устанавливает требования к системе менеджмента безопасности, включая аспекты, относящиеся к цепи поставок.

Настоящий стандарт применим к организациям всех типов и размеров (например, коммерческим предприятиям, правительственным или другим государственным учреждениям и некоммерческим организациям), которые намерены создать, внедрить, поддерживать и улучшать систему менеджмента безопасности. Он обеспечивает целостный и общий подход и не является отраслевым или секторальным.

Настоящий стандарт может использоваться на протяжении всего периода существования организации и применяться к любой деятельности, внутренней или внешней, на всех уровнях.

2 Нормативные ссылки

Для применения настоящего стандарта необходим следующий ссылочный стандарт. Для датированных ссылок применяют только указанное издание. Для недатированных ссылок применяют последнее издание ссылочного документа (включая любые изменения).

ISO 22300, Security and resilience – Vocabulary (Безопасность и устойчивость. Словарь)

3 Термины и определения

В настоящем стандарте применяют термины, установленные в ISO 22300, а также следующие термины с соответствующими определениями.

ISO и IEC поддерживают терминологические базы данных для использования в стандартизации по следующим адресам:

- платформа интернет-поиска ISO: https://www.iso.org/obp;
- электропедия IEC: http://www.electropedia.org/.

3.1 организация (organization): Лицо или группа персонала, которые имеют свои собственные функции с обязанностями, полномочия и взаимоотношения для достижения своих **целей (3.7)**.

Примечание 1 – Концепция организации включает, но не ограничена: индивидуальным предпринимателем, компанией, корпорацией, фирмой, предприятием, органом, товариществом, благотворительной организацией или учреждением, а также их частями или их комбинацией, независимо от того, имеют они статус юридического лица или нет, являются государственными или частными.

Примечание 2 – Если организация является частью более крупной организации, термин «организация» относится только к той части более крупной организации, которая находится в области применения **системы менеджмента безопасности (3.5)**.

3.2 заинтересованная сторона (interested party, предпочтительный термин); стейкхолдер (stakeholder, допускаемый термин): Лицо или **организация (3.1)**, которые могут воздействовать, подвергаться воздействию или воспринимать себя подверженными воздействию решения или деятельности.

3.3 высшее руководство (top management): Лицо или группа персонала, которая направляет **организацию (3.1)** и управляет ею на высшем уровне.

Примечание 1 – Высшее руководство имеет право делегировать полномочия и предоставлять ресурсы в пределах организации.

Примечание 2 – Если область применения **системы менеджмента (3.4)** распространяется только на часть организации, то высшее руководство относится к тем, кто направляет эту часть организации и управляет ею.

3.4 система менеджмента (management system): Набор взаимосвязанных или взаимодействующих элементов **организации (3.1)** для установления **политик (3.6)** и **целей (3.7)**, а также **процессов (3.9)** для достижения этих целей.

Примечание 1 – Система менеджмента может рассматривать одну дисциплину или несколько дисциплин.

Примечание 2 – Элементы системы менеджмента включают структуру организации, роли и обязанности, планирование, функционирование.

3.5 система менеджмента безопасности (security management system): Система скоординированных **политик (3.6)**, **процессов (3.9)** и практик, с помощью которых организация осуществляет менеджмент своих **целей (3.7)** в области безопасности.

3.6 политика (policy): Намерения и направления **организации (3.1)**, официально выраженные ее **высшим руководством (3.3).**

3.7 цель (objective): Результат, который будет достигаться.

Примечание 1 – Цель может быть стратегической, тактической или операционной.

Примечание 2 – Цели могут относиться к различным дисциплинам (например, финансовые цели, цели в области промышленной безопасности и здоровья, цели в области окружающей среды). Они могут быть, например общеорганизационными или специфическими для проекта, продукции и **процесса (3.9)**.

Примечание 3 – Цель может быть выражена другим способом, например, как предполагаемый результат, намерение, операционный критерий, как цель в области безопасности или при помощи других слов, имеющих аналогичное значение (в английском языке), (например, aim (цель), goal (цель) или target (задача)).

Примечание 4 – В контексте **систем менеджмента безопасности (3.5)** цели в области безопасности устанавливаются **организацией (3.1)**, согласованы с **политикой (3.6)** в области безопасности для достижения конкретных результатов.

3.8 риск (risk): Воздействие неопределенности на **цели (3.7)**.

Примечание 1 – Воздействие – это отклонение от того, что ожидается. Оно может быть положительным, отрицательным или и тем, и другим, и может устранять, создавать или приводить к возможностям и угрозам.

Примечание 2 – Цели могут иметь различные аспекты и категории и могут применяться на разных уровнях.

Примечание 3 – Риск обычно выражается в терминах источников риска, потенциальных событий, их последствий и вероятности.

3.9 процесс (process): Набор взаимосвязанных или взаимодействующих видов деятельности, которые используют входы для поставки намеченного результата.

Примечание 1 – В зависимости от контекста намеченный результат процесса называют выходом, продукцией или услугой.

3.10 компетентность (competence): Способность применять знания и навыки для достижения намеченных результатов.

3.11 документированная информация (documented information): Информация, требующая управления и поддержки **организации (3.1)**, а также носитель, на котором она содержится.

Примечание 1 – Документированная информация может быть представлена в любом формате и на любом носителе и получена из любого источника.

Примечание 2 – Документированная информация может относиться к:

- **системе менеджмента (3.4)**, включая связанные **процессы (3.9)**;
- информации, созданной для работы организации (документация);
- свидетельству достигнутых результатов (записи).

3.12 пригодность (performance): Измеримый результат.

Примечание 1 – Пригодность может относиться либо к количественным, либо к качественным наблюдениям.

Примечание 2 – Пригодность может относиться к менеджменту деятельности, **процессов (3.9)**, продукции, услуг, систем или **организаций (3.1)**.

3.13 постоянное улучшение (continual improvement): Повторяющаяся деятельность по повышению **пригодности (3.12)**.

3.14 результативность (effectiveness): Степень реализации запланированной деятельности и достижения запланированных результатов.

3.15 требование (requirement): Потребность или ожидание, которое устанавливается, обычно предполагается или является обязательным.

Примечание 1 – «Обычно предполагается» означает, что это обычная или общепринятая практика **организации (3.1)** и **заинтересованных сторон (3.2)**, когда рассматриваемые потребности или ожидания являются предполагаемыми.

Примечание 2 – Установленным требованием является такое требование, которое сформулировано, например, в **документированной информации (3.11)**.

3.16 соответствие (conformity): Выполнение **требования (3.15)**.

3.17 несоответствие (nonconformity): Невыполнение **требования (3.15)**.

3.18 корректирующее действие (corrective action): Действие, предпринятое для устранения причин (ы) **несоответствия (3.17)** и предупреждения повторного его возникновения.

3.19 аудит (audit): Систематический и независимый **процесс (3.9)** получения объективных свидетельств и объективного их оценивания для определения степени выполнения критериев аудита.

Примечание 1 – Аудит может быть внутренним аудитом (первой стороной) или внешним аудитом (второй стороной или третьей стороной), а также комбинированным аудитом (объединяющим две или более дисциплин).

Примечание 2 – Внутренний аудит проводится самой **организацией (3.1**) или внешней стороной по ее поручению.

Примечание 3 – «Свидетельства аудита» и «критерии аудита» определены в ISO 19011.

3.20 измерение (measurement): **Процесс (3.9)** определения значения.

3.21 мониторинг (monitoring): Определение статуса системы, **процесса (3.9)** или деятельности.

Примечание 1 – Для определения статуса может возникнуть необходимость проверять, осуществлять надзор или критично наблюдать.

4 Контекст организации

4.1 Понимание организации и ее контекста

Организация должна определить внешние и внутренние факторы, которые относятся к ее назначению и которые влияют на ее способность достичь намеченного (ых) результата (ов) ее системы менеджмента безопасности, включая требования ее цепи поставок.

4.2 Понимание потребностей и ожиданий заинтересованных сторон

4.2.1 Общие положения

Организация должна определить:

- заинтересованные стороны, которые имеют отношение к системе менеджмента безопасности;
- соответствующие требования этих заинтересованных сторон;
- какие из этих требований будут выполняться с помощью системы менеджмента безопасности.

4.2.2 Правовые, нормативные и другие требования

Организация должна:

a) внедрить и поддерживать процесс для идентификации, доступа и оценки применимых правовых, нормативных и других требований, связанных с ее безопасностью;

b) обеспечить учет этих применимых правовых, нормативных и других требований при внедрении и поддержании ее системы менеджмента безопасности;

c) документировать эту информацию и сохранять ее в актуальном состоянии;

d) сообщать эту информацию соответствующим заинтересованным сторонам по мере необходимости.

4.2.3 Принципы

4.2.3.1 Общие положения

Назначением менеджмента безопасности в организации является создание и, в частности, защита ценности.

Организации следует применять принципы, приведенные на рисунке 2 и описанные в 4.2.3.2 – 4.2.3.9.

Рисунок 2 – Принципы

4.2.3.2 Лидерство

Лидерам следует устанавливать на всех уровнях единство назначения и направления. Им следует создавать условия для согласования стратегий, политики, процессов и ресурсов организации для достижения целей. В разделе 5 разъясняются требования к этому принципу.

4.2.3.3 Структурированный и комплексный подход к процессу, основанный на наилучшей доступной информации

Структурированный и комплексный подход к менеджменту безопасности, включая цепь поставок, должен способствовать достижению последовательных и сопоставимых результатов, которые достигаются более эффективно и результативно, когда деятельность понимается и управляется как взаимосвязанные процессы, функционирующие как целостная система.

4.2.3.4 Индивидуальный подход

Следует, чтобы система менеджмента безопасности была индивидуальной и соразмерной внешнему и внутреннему контексту и потребностям организации. Ей следует быть связанной с ее целями.

4.2.3.5 Инклюзивная привлеченность людей

Организации следует надлежащим образом и своевременно вовлекать заинтересованные стороны. Ей следует надлежащим образом учитывать их знания, взгляды и восприятие для улучшения осведомленности и содействия информированному менеджменту безопасности. Организации следует обеспечить уважение и участие каждого на всех уровнях.

4.2.3.6 Интегрированный подход

Менеджмент безопасности является интегрированной частью всей организационной деятельности. Его следует интегрировать со всеми другими системами менеджмента организации.

Менеджмент риска организации (формальный, неформальный или интуитивный) следует интегрировать в систему менеджмента безопасности.

4.2.3.7 Динамичность и постоянное улучшение

Организации следует постоянно фокусироваться на улучшении через обучение и опыт, чтобы поддерживать уровень пригодности, реагировать на изменения и создавать новые возможности по мере изменения внешнего и внутреннего контекста организации.

4.2.3.8 Учет человеческих и культурных факторов

Человеческое поведение и культура существенно влияют на все аспекты менеджмента безопасности и должны учитываться на каждом уровне и стадии. Решения следует основывать на анализе и оценивании данных и информации для обеспечения большей объективности, уверенности в принятии

решений и большей вероятности получения желаемых результатов. Следует учитывать индивидуальное восприятие.

4.2.3.9 Менеджмент взаимоотношений

Для достижения устойчивого успеха организации следует осуществлять менеджмент своих взаимоотношений со всеми соответствующими заинтересованными сторонами, поскольку они могут повлиять на пригодность организации.

4.3 Определение области применения системы менеджмента безопасности

Организация должна определить границы и применимость системы менеджмента безопасности, чтобы установить ее область применения.

При определении этой области применения организация должна рассматривать:

- внешние и внутренние факторы, указанные в 4.1;
- требования, указанные в 4.2.

Область применения должна быть доступна в виде документированной информации.

Если организация решает, чтобы любой процесс, влияющий на соответствие ее системе менеджмента безопасности, предоставлялся извне, организация должна обеспечить управление такими процессами. Необходимые средства управления и обязанности за такие процессы, предоставляемые извне, должны быть идентифицированы в системе менеджмента безопасности.

4.4 Система менеджмента безопасности

Организация должна разработать, внедрить, поддерживать и постоянно улучшать систему менеджмента безопасности, включая необходимые процессы и их взаимодействие, в соответствии с требованиями настоящего стандарта.

5 Лидерство

5.1 Лидерство и приверженность

Высшее руководство должно демонстрировать лидерство и приверженность по отношению к системе менеджмента безопасности посредством:

- обеспечения того, что политика в области безопасности и цели в области безопасности установлены и согласованы со стратегическим направлением организации;
- обеспечения идентификации и мониторинга требований и ожиданий заинтересованных сторон организации, а также своевременного принятия соответствующих действий по управлению этими ожиданиями для обеспечения интеграции требований системы менеджмента безопасности в бизнес-процессы организации;
- обеспечения интеграции требований системы менеджмента безопасности в бизнес-процессы организации;
- обеспечения того, чтобы ресурсы, необходимые для системы менеджмента безопасности, были доступны;
- доведения до сведения важности результативного менеджмента безопасности и соответствия требованиям системы менеджмента безопасности;
- обеспечения того, чтобы система менеджмента безопасности достигала своих намеченных результатов;
- обеспечения жизнеспособности целей, задач и программ менеджмента безопасности;
- обеспечения того, чтобы любые программы безопасности, разработанные другими подразделениями организации, дополняли систему менеджмента безопасности;
- направления и поддержки персонала, который вносит вклад в результативность системы менеджмента безопасности;
- содействия постоянному улучшению системы менеджмента безопасности организации;
- поддержки других соответствующих ролей для демонстрации ими лидерства применительно к областям их обязанностей.

Примечание – Ссылка на «бизнес» в настоящем стандарте может быть интерпретирована самым широким образом, чтобы обозначить те виды деятельности, которые являются основными для намерений существования организации.

5.2 Политика в области безопасности

5.2.1 Установление политики в области безопасности

Высшее руководство должно установить политику в области безопасности, которая:

a) соответствует предназначению организации;

b) предоставляет основу для установки целей в области безопасности;

c) включает обязательство соответствовать применимым требованиям;

d) включает обязательство постоянно улучшать систему менеджмента безопасности;

e) учитывает негативное воздействие, которое политика в области безопасности, цели, задачи, программы и т.д. могут оказать на другие аспекты деятельности организации.

5.2.2 Требования к политике в области безопасности

Политика в области безопасности должна:

- соответствовать другим политикам организации;
- соответствовать общей оценке рисков безопасности организации;
- предусматривать ее пересмотр в случае приобретения или слияния с другими организациями или других изменений в области деятельности организации, которые могут повлиять на непрерывность или актуальность системы менеджмента безопасности;
- описывать и распределять первичную подотчетность и обязанности за итоговые выходы;
- быть доступной в виде документированной информации;
- быть доведена до сведения в организации;
- быть доступной для заинтересованных сторон, при необходимости.

Примечание – Организации могут выбрать подробную политику менеджмента безопасности для внутреннего использования, которая обеспечит достаточную информацию и направление для управляемой системой менеджмента безопасности (части которой могут быть конфиденциальными), и иметь обобщенную (неконфиденциальную) версию, содержащую общие цели для распространения среди заинтересованных сторон.

5.3 Роли, обязанности и полномочия в организации

Высшее руководство должно обеспечивать, чтобы обязанности и полномочия в отношении соответствующих ролей назначались, доводились до сведения в организации.

Высшее руководство должно назначить обязанности и полномочия для:

a) обеспечения того, чтобы система менеджмента безопасности соответствовала требованиям настоящего стандарта;

b) предоставления отчетов о пригодности системы менеджмента безопасности перед высшим руководством.

6 Планирование

6.1 Действия по рассмотрению рисков и возможностей

6.1.1 Общие положения

При планировании системы менеджмента безопасности организация должна рассмотреть факторы, приведенные в 4.1, и требования, приведенные в 4.2, и определить риски и возможности, которые необходимо рассмотреть, чтобы:

- гарантировать, что система менеджмента безопасности может достигать намеченных (ых) результата (ов);
- предупредить или снизить нежелательные последствия;
- достигать постоянно улучшения.

Организация должна планировать:

a) действия по рассмотрению этих рисков и возможностей;

b) то, как:
   - интегрировать и внедрять эти действия в процессы системы менеджмента безопасности;
   - оценивать результативность этих действий.

Целью менеджмента рисков является создание и защита ценности. Менеджмент риска должен быть интегрирован в систему менеджмента безопасности. Риски, связанные с безопасностью организации и ее заинтересованных сторон, рассматриваются в 8.3.

6.1.2 Определение рисков, связанных с безопасностью, и идентификация возможностей

Определение рисков, связанных с безопасностью, а также идентификация и использование возможностей требует проактивной оценки рисков, которая должна включать рассмотрение (но не ограничивается ими):

a) физических или функциональных отказов, а также злонамеренных или преступных действий;

b) факторов окружающей среды, человеческих и культурных факторов и других внутренних или внешних контекстов, включая факторы вне управления организации, влияющие на безопасность организации;

c) вопросов проектирования, установки, обслуживания и замены оборудования для обеспечения безопасности;

d) менеджмента информации, данных, знаний и коммуникаций организации;

e) информации, связанной с угрозами и уязвимостями безопасности;

f) взаимозависимости между поставщиками.

6.1.3 Рассмотрение рисков, связанных с безопасностью, и использование возможностей

Оценивание идентифицированного риска, связанного с безопасностью, должно обеспечить вход для (но не ограничиваться этим):

a) общего менеджмента риска организации;

b) обработки риска;

c) достижения целей менеджмента безопасности;

d) процессов менеджмента безопасности;

e) проектирования, спецификации и внедрения системы менеджмента безопасности;

f) идентификации адекватных ресурсов, включая персонал;

g) идентификации потребностей в подготовки и требуемого уровня компетентности.

6.2 Цели в области безопасности и планирование их достижения

6.2.1 Установление целей в области безопасности

Организация должна установить цели в области безопасности для соответствующих функций и уровней.

Цели в области безопасности должны:

a) быть согласованными с политикой в области безопасности;

b) быть измеримыми (если практически возможно);

c) принимать во внимание применимые требования;

d) подлежать мониторингу;

e) доводиться до сведения;

f) обновляться при необходимости;

g) быть доступны в виде документированной информации.

6.2.2 Определение целей в области безопасности

При планировании достижения своих целей в области безопасности организация должна определить:

- что будет сделано;
- какие ресурсы потребуются;
- кто будет ответственным;
- когда это будет завершено;
- каким образом будут оцениваться результаты.

При установлении и пересмотре целей в области безопасности организация должна принимать во внимание:

a) технологические, человеческие, административные и другие факторы;

b) мнения и воздействия на соответствующие заинтересованные стороны.

Цели в области безопасности должны соответствовать стремлению организации к постоянному улучшению.

6.3 Планирование изменений

Когда организацией определена необходимость в изменениях системы менеджмента безопасности, включая те, которые идентифицированы в разделе 10, эти изменения должны проводиться в плановом порядке.

Организация должна рассмотреть:

a) назначение изменений и их потенциальные последствия;

b) целостность системы менеджмента безопасности;
c) доступность ресурсов;
d) распределение или перераспределение обязанностей и полномочий.

7 Поддержка

7.1 Ресурсы

Организация должна определить и предоставить ресурсы, необходимые для разработки, внедрения, поддержания и постоянного улучшения системы менеджмента безопасности.

7.2 Компетентность

Организация должна:

– определить необходимую компетентность персонала, осуществляющего работу под ее управлением, которая воздействует на пригодность ее безопасности;

– обеспечить, чтобы этот персонал обладал компетентностью на основе соответствующего образования, подготовки или опыта и прошел соответствующую проверку службы безопасности;

– если применимо, осуществлять действия по приобретению необходимой компетентности и оценивать результативность предпринятых действий.

Соответствующая документированная информация должна быть доступна в качестве свидетельства компетентности.

Примечание – Применяемые действия могут включать, например, предоставление подготовки, менторинг или перераспределение сотрудников, наем или заключение контрактов с компетентным персоналом.

7.3 Осведомленность

Персонал, работающий под управлением организации, должен быть осведомлен о:

– политике в области безопасности;

– его вкладе в результативность системы менеджмента безопасности, включая выгоды от улучшения пригодности;

– последствиях несоответствий требованиям системы менеджмента безопасности;

– своих ролях и обязанностях в достижении соответствия политике и процедурам менеджмента безопасности и требованиям системы менеджмента безопасности, включая требования по готовности к чрезвычайным ситуациям и реагированию на них.

7.4 Коммуникации

Организация должна определить внутренние и внешние коммуникации, относящиеся к системе менеджмента безопасности, включая то:

– о чем будут осуществляться коммуникации;
– когда будут осуществляться коммуникации;
– с кем будут осуществляться коммуникации;
– как будут осуществляться коммуникации;
– какой будет уровень закрытости информации до ее распространения.

7.5 Документированная информация

7.5.1 Общие положения

Система менеджмента безопасности организации должна включать:

a) документированную информацию, требуемую настоящим стандартом;
b) документированную информацию, определенную организацией как необходимую для результативности системы менеджмента безопасности.

Документированная информация должна описывать обязанности и полномочия по достижению целей и задач менеджмента безопасности, включая средства и сроки достижения этих целей и задач.

Примечание – Объем документированной информации системы менеджмента безопасности одной организации может отличаться от другой в зависимости от:

– размера организации и вида ее деятельности, процессов, продукции и услуг;
– сложности процессов и их взаимодействия;
– компетентности персонала.

Организация должна определить ценность информации, установить требуемый уровень целостности и средства управления безопасности для предотвращения несанкционированного доступа.

7.5.2 Создание и обновление документированной информации

При создании и обновлении документированной информации организация должна обеспечить:

– идентификацию и описание (например, наименование, дата, автор или учетный номер);

– формат (например, язык, версия программного обеспечения, графика) и носитель (например, бумажный или электронный);

– анализ и одобрение информации с точки зрения приемлемости и адекватности.

7.5.3 Управление документированной информацией

Документированная информация, требуемая системой менеджмента безопасности и настоящим стандартом, должна находиться под управлением для обеспечения того, что:

a) она доступна и приемлема для использования, где и когда это необходимо;

b) она адекватно защищена (например, от нарушения конфиденциальности, ненадлежащего использования или нарушения целостности);

c) она периодически анализируется и пересматривается по мере необходимости, и одобряется уполномоченным персоналом на предмет адекватности;

d) устаревшие документы, данные и информация незамедлительно удаляются из всех пунктов выдачи и пунктов использования или иным образом обеспечивают защиту от непреднамеренного использования;

e) архивные документы, данные и информация, сохраняемые в юридических целях или в целях сохранения знаний, или и то, и другое, соответствующим образом идентифицируют.

Для управления документированной информацией организация должна, если применимо, рассмотреть следующую деятельность:

– распределение, доступ, восстановление и использование;

– накопление и обеспечение сохранности, включая сохранение разборчивости;

– управление изменениями (например, управление версиями);

– хранение и размещение.

Документированная информация внешнего происхождения, определенная организацией как необходимая для планирования и функционирования системы менеджмента безопасности, должна быть соответствующим образом идентифицирована и управляема.

Примечание – Доступ может предполагать разрешение только ознакомиться с документированной информацией или разрешение и полномочия ознакомиться и изменить документированную информацию.

8 Операционная деятельность

8.1 Планирование и управление деятельностью

Организация должна планировать, внедрять и управлять процессами, необходимыми для выполнения требований по предоставлению продукции и услуг, а также внедрению действий, определенных в разделе 6, посредством:

– установления критериев для процессов;

– внедрения средств управления процессами в соответствии с установленными критериями.

Документированная информация должна быть доступна в объеме, необходимом для уверенности в том, что процессы были выполнены в соответствии с планом.

8.2 Идентификация процессов и видов деятельности

Организация должна идентифицировать те процессы и виды деятельности, которые необходимы для достижения:

a) соответствия своей политике в области безопасности;

b) соответствия правовым, законодательным и нормативным требованиям безопасности;

c) ее целей менеджмента безопасности;

d) поставки ее системы менеджмента безопасности;

e) требуемого уровня безопасности цепи поставок.

8.3 Оценка и обработка риска

Организация должна внедрить и поддерживать процесс оценки и обработки риска.

Примечание – Процесс оценки и обработки риска рассматривается в ISO 31000.

Организации следует:

a) идентифицировать свои риски, связанные с безопасностью, определяя их приоритезацию по отношению к ресурсам, необходимым для менеджмента безопасности;

b) анализировать и оценивать идентифицированные риски;

c) определить, какие риски требуют обработки;

d) выбрать и внедрить варианты для устранения этих рисков;

e) подготовить и внедрить планы по обработке риска.

Примечание – Риски в этом подразделе относятся к безопасности организации и ее заинтересованных сторон. Риски и возможности, связанные с результативностью системы менеджмента, рассматриваются в 6.1.

8.4 Средства управления

Процессы, перечисленные в 8.2, должны включать средства управления для менеджмента человеческих ресурсов, а также проектирование, установку, эксплуатацию, переоборудование и модификацию связанных с безопасностью элементов оборудования, приборов и информационных технологий при необходимости. При пересмотре существующих или введении новых механизмов, которые могут воздействовать на менеджмент безопасности, до их внедрения организация должна рассмотреть риски, связанные с безопасностью. Новые или пересмотренные механизмы, которые должны быть рассмотрены, должны включать:

a) пересмотренную организационную структуру, роли или обязанности;

b) подготовку, осведомленность и менеджмент человеческих ресурсов;

c) пересмотренную политику, цели, задачи или программы менеджмента безопасности;

d) пересмотренные процессы и процедуры;

e) внедрение новой инфраструктуры, оборудования или технологии безопасности, которые могут включать аппаратное и/или программное обеспечение;

f) введение новых подрядчиков, поставщиков или персонала при необходимости;

g) требования к обеспечению безопасности внешних поставщиков.

Организация должна управлять запланированными изменениями и анализировать последствия непреднамеренных изменений, принимая при необходимости действия по смягчению любых негативных последствий.

Организация должна обеспечить управление предоставляемых извне процессами, продукцией или услугой, имеющих отношение к системе менеджмента безопасности.

8.5 Стратегии, процедуры, процессы и методы обеспечения безопасности

8.5.1 Идентификация и выбор стратегий и методов обеспечения безопасности

Организации следует внедрить и поддерживать систематические процессы анализа уязвимостей и угроз, связанных с безопасностью. На основе анализа уязвимостей и угроз и последующей оценки рисков организации следует идентифицировать и выбрать стратегию в области безопасности, которая включает в себя одну или несколько процедур, процессов и методов обеспечения безопасности.

Следует, чтобы идентификация основывалась на том, в какой степени стратегии, процедуры, процессы и методы обеспечения безопасности:

a) поддерживают безопасность организации;

b) снижают вероятность возникновения уязвимости безопасности;

c) снижают вероятность актуализации угрозы;

d) сокращают период любых недостатков методов обеспечения безопасности и ограничивают их воздействие;

e) предусматривают наличие адекватных ресурсов.

Следует, чтобы выбор был основан на том, в какой степени стратегии, процессы и методы обеспечения безопасности:

- соответствуют требованиям по защите безопасности организации;
- учитывают величину и тип риска, который организация может принять или не принять;
- учитывают связанные с ними затраты и выгоды.

8.5.2 Требования к ресурсам

Организация должна определить требования к ресурсам для внедрения выбранных процедур, процессов и методов обеспечения безопасности.

8.5.3 Внедрение методов обеспечения безопасности

Организация должна внедрить и поддерживать выбранные методы обеспечения безопасности.

8.6 Планы безопасности

8.6.1 Общие положения

Организация должна разработать и задокументировать планы и процедуры обеспечения безопасности на основе выбранных стратегий и методов обеспечения безопасности. Организация должна внедрить и поддерживать структуру реагирования, которая позволит своевременно и результативно предупреждать и сообщать соответствующим заинтересованным сторонам об уязвимостях, связанных с безопасностью, и о неминуемых угрозах безопасности или текущих нарушениях безопасности. Структура реагирования должна предусматривать планы и процедуры менеджмента организации во время неминуемой угрозы безопасности или продолжающегося нарушения безопасности.

8.6.2 Структура реагирования

Организация должна внедрить и поддерживать структуру, идентифицирующую назначенное лицо или одну или несколько команд, ответственных за реагирование на уязвимости и угрозы, связанные с безопасностью. Роли и обязанности назначенного лица или каждой команды, а также взаимоотношения между ними должны быть четко идентифицированы, доведены до сведения и документированы.

В совокупности команды должны быть компетентны для:

a) оценки характера и степени угрозы для безопасности и ее потенциального воздействия;

b) оценки воздействия по заранее определенным пороговым значениям, которые обосновывают инициирование формального реагирования в области безопасности;

c) активации соответствующего реагирования в области безопасности;

d) планирования действий, которые необходимо предпринять;

e) установления приоритетов, используя безопасность жизнедеятельности в качестве первого приоритета;

f) осуществления мониторинга последствий любых вариаций в уязвимостях, связанных с безопасностью, изменений в намерениях и возможностях субъектов угроз или нарушений безопасности, а также реагирование организации;

g) активации методов обеспечения безопасности;

h) обмена информацией с соответствующими заинтересованными сторонами, органами власти и средствами массовой информации;

i) внесения вклада в план коммуникаций с руководством по коммуникации.

Для каждого назначенного лица или команды следует иметь:

– идентифицированный штат, включая заместителей с необходимыми обязанностями, полномочиями и компетентностью для выполнения назначенной роли;

– документированные процедуры для руководства их действиями, включая процедуры активации, эксплуатации, координации и коммуникации реагирования.

8.6.3 Предупреждение и коммуникация

Организации следует документировать и поддерживать процедуры для:

a) обмена информацией внутри и за пределами организации с соответствующими заинтересованными сторонами, включая о чем, когда, с кем и как проходит коммуникация;

Примечание – Организация может документировать и поддерживать процедуры того, как и при каких обстоятельствах организация осуществляет обмен информацией с сотрудниками и их контактами в чрезвычайных ситуациях.

b) получения, документирования и реагирования на сообщения от заинтересованных сторон, включая любую национальную или региональную консультативную систему по рискам или ее эквивалент;

c) обеспечения доступности средств коммуникации во время нарушения безопасности, возникновения уязвимости или угрозы;

d) содействия структурированной коммуникации с лицами, реагирующими на угрозы и/или нарушения безопасности;

e) предоставления подробной информации о реагировании средств массовой информации организации на нарушения безопасности, включая стратегию коммуникации;

f) регистрации деталей нарушения безопасности, предпринятых действий и принятых решений.

Если применимо, следует также рассмотреть и внедрить следующее:

– оповещение заинтересованных сторон, потенциально затронутых фактическим или предстоящим нарушением безопасности;

– обеспечение надлежащей координации и связи между многочисленными реагирующими организациями.

Процедуры оповещения и коммуникации должны отрабатываться в рамках программы испытания и подготовки организации.

8.6.4 Содержание планов безопасности

Организация должна документировать и поддерживать планы безопасности. Следует, чтобы эти планы содержали руководство и информацию для оказания помощи командам по реагированию на уязвимость, угрозу и/или нарушение безопасности, а также для оказания помощи организации в реагировании и восстановлении ее безопасности.

В совокупности следует, чтобы планы безопасности содержали:

a) подробное описание действий, которые предпримут команды для:

1) продолжения или восстановления согласованного статуса безопасности;

2) мониторинга воздействия фактических или надвигающихся угроз, уязвимостей или нарушений безопасности и реагирования организации на них;

b) ссылку на заранее определенный порог (и) и процесс активации реагирования;

c) процедуры по восстановлению безопасности организации;

d) подробные описания для менеджмента непосредственных последствий уязвимости и угрозы безопасности или фактического или предстоящего нарушения безопасности с учетом:

1) благополучия персонала;

2) ценности активов, информации и персонала, которые могут быть скомпрометированы;

3) предотвращения (дальнейшей) потери или недоступности основной деятельности.

Следует, чтобы каждый план включал:

– его назначение, область применения и цели;

– роли и обязанности команды, которая будет внедрять план;

– действия по внедрению решений;

– информацию, необходимую для активации (включая критерии активации), работы, координации и передачи информации о действиях команды;

– внутренние и внешние взаимозависимости;

– требования к ресурсам;

– требования к отчетности;

– процесс свертывания деятельности.

Следует, чтобы каждый план был пригодным к использованию и доступен в то время и в том месте, в котором он требуется.

8.6.5 Восстановление

Организация должна иметь документированные процессы для восстановления безопасности организации из любых временных мер, принятых до, во время и после нарушения безопасности.

9 Оценивание пригодности

9.1 Мониторинг, измерения, анализ и оценивание

Организация должна определить:

– мониторинг и измерения того, что необходимо осуществлять;

– методы мониторинга, измерений, анализа и оценивания, если применимо, для обеспечения валидированных результатов;

– когда должны выполняться мониторинг и измерения;

– когда результаты мониторинга и измерений должны быть проанализированы и оценены.

Документированная информация должна быть доступна в качестве свидетельства полученных результатов.

Организация должна оценивать пригодность и результативность системы менеджмента безопасности.

9.2 Внутренний аудит

9.2.1 Общие положения

Организация должна проводить внутренние аудиты через запланированные интервалы времени для предоставления информации о том, что система менеджмента безопасности:

a) соответствует:
   1) требованиям организации к своей системе менеджмента качества;
   2) требованиям настоящего стандарта;
b) результативно внедрена и поддерживается.

9.2.2 Программа внутреннего аудита

Организация должна планировать, устанавливать, выполнять и поддерживать программу (ы) аудита, которая (ые) включает (ют) частоту, методы, обязанности, планируемые требования и отчетность.

При разработке программ (ы) внутреннего аудита организация должна учитывать важность соответствующих процессов и результаты предыдущих аудитов.

Организация должна:

a) определять для каждого аудита критерии и область применения аудита;

b) отбирать аудиторов и проводить аудит так, чтобы была обеспечена объективность и беспристрастность процесса аудита;

c) обеспечить, чтобы результаты аудитов были доведены до сведения соответствующих менеджеров;

d) убедиться, что оборудование и персонал для обеспечения безопасности размещены надлежащим образом;

e) обеспечить, чтобы все необходимые корректирующие действия предпринимались без неоправданной задержки для устранения обнаруженных несоответствий и их причин;

f) обеспечить, чтобы последующие действия по аудиту включали верификацию предпринятых действий и отчетность о результатах верификации.

Документированная информация должна быть доступна в качестве свидетельства внедрения программ (ы) аудитов и результатов аудита.

Программа аудита, включая любой график, должна быть основана на результатах оценки рисков деятельности организации и результатах предыдущих аудитов. Процедуры аудита должны охватывать объем, частоту, методологии и компетенции, а также обязанности и требования к проведению аудита и представлению результатов.

9.3 Анализ со стороны руководства

9.3.1 Общие положения

Высшее руководство должно через запланированные интервалы анализировать систему менеджмента безопасности организации, чтобы обеспечить ее постоянную приемлемость, адекватность, результативность.

Организация должна рассмотреть результаты анализа и оценивания, а также выходы анализа со стороны руководства, чтобы определить, есть ли потребности или возможности, относящиеся к бизнесу или системе менеджмента безопасности, которые должны быть рассмотрены как часть постоянного улучшения.

Примечание – Организация может использовать процессы системы менеджмента безопасности, такие как лидерство, планирование и оценивание пригодности, для достижения улучшения.

9.3.2 Входы анализа со стороны руководства

Анализ со стороны руководства должен включать:

a) статус действий, осуществляемых по итогам предыдущих анализов со стороны руководства;

b) изменения в соответствующих внешних и внутренних факторах, касающихся системы менеджмента безопасности;

c) изменения в потребностях и ожиданиях заинтересованных сторон, имеющих отношение к системе менеджмента безопасности;

d) информацию о пригодности безопасности, включая тренды в:
   1) несоответствиях и корректирующих действиях;
   2) результатах мониторинга и измерений;
   3) результатах аудитов;

e) возможности для постоянного улучшения;

f) результаты аудитов и оценивания соблюдения требований законодательства и других требований, которым подчиняется организация;

g) сообщение(я) от внешних заинтересованных сторон, включая жалобы;

h) пригодность безопасности организации;

i) степень выполнения целей и задач;
j) статус корректирующих действий;
k) последующие действия по результатам предыдущих анализов со стороны руководства;
l) изменение обстоятельств, включая изменения в правовых, нормативных и других требованиях (см. 4.2.2), связанных с аспектами безопасности;
m) рекомендации для улучшения.

9.3.3 Результаты анализа со стороны руководства

Результаты анализа со стороны руководства должны включать решения, связанные с возможностями постоянного улучшения и любой необходимостью внесения изменений в систему менеджмента безопасности.

Документированная информация должна быть доступна в качестве свидетельства полученных результатов анализа со стороны руководства.

10 Улучшение

10.1 Постоянное улучшение

Организация должна постоянно улучшать приемлемость, адекватность и результативность системы менеджмента безопасности. Организации следует активно искать возможности для улучшения, даже если это не вызвано уязвимостями, связанными с безопасностью, и непосредственными угрозами безопасности или продолжающимися нарушениями безопасности, соответствующим заинтересованным сторонам.

10.2 Несоответствия и корректирующие действия

Если возникает несоответствие, организация должна:

a) отреагировать на несоответствие и, если применимо:
   1) предпринять действия по его управлению и коррекции;
   2) бороться с последствиями;
b) оценить необходимость действий по устранению причины (причин) несоответствия, с тем чтобы оно не повторилось или не возникло в другом месте, посредством:
   1) рассмотрения и анализа несоответствия;
   2) определения причин несоответствия;
   3) определения того, существуют ли аналогичные несоответствия и могут ли они потенциально возникнуть;
c) выполнить все необходимые действия;
d) проанализировать результативность каждого выполненного корректирующего действия;
e) внести, при необходимости, изменения в систему менеджмента безопасности.

Корректирующие действия должны соответствовать последствиям выявленных несоответствий.

Документированная информация должна быть доступна в качестве свидетельства:

- характера несоответствий и любых последующих предпринятых действий;
- результатов каждого корректирующего действия;
- расследования, связанного с безопасностью:
  - отказов, включая потенциально опасные ситуации и ложные тревоги;
  - инцидентов и чрезвычайных ситуаций;
  - несоответствий;
- принятия действий по смягчению любых последствий, возникающих в результате таких отказов, инцидентов или несоответствий.

Процедуры должны требовать, чтобы все предлагаемые корректирующие действия рассматривались в процессе оценки риска, связанного с безопасностью, до их внедрения, за исключением случаев, когда немедленное внедрение предотвращает неминуемую угрозу для жизни или общественной безопасности.

Любые корректирующие действия, предпринятые для устранения причин фактических и потенциальных несоответствий, должны соответствовать масштабу проблем и соизмеряться с вероятными рисками, связанными с менеджментом безопасности.

Библиография

[1] ISO 9001, Quality management systems – Requirements (Системы менеджмента качества. Требования)

[2] ISO 14001, Environmental management systems – Requirements with guidance for use (Системы экологического менеджмента. Требования и руководство по применению)

[3] ISO 19011, Guidelines for auditing management systems (Руководящие указания по аудиту систем менеджмента)

[4] ISO 22301, Security and resilience – Business continuity management systems – Requirements (Безопасность и устойчивость. Системы менеджмента непрерывности бизнеса. Требования)

[5] ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements (Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования)

[6] ISO 28001, Security management systems for the supply chain – Best practices for implementing supply chain security, assessments and plans – Requirements and guidance (Системы менеджмента безопасности цепи поставок. Наилучшие методы обеспечения безопасности в цепи поставок, оценки и планы. Требования и руководящие указания)

[7] ISO 28002, Security management systems for the supply chain – Development of resilience in the supply chain – Requirements with guidance for use (Системы менеджмента безопасности цепи поставок. Развитие устойчивости в цепи поставок. Требования и руководство по применению)

[8] ISO 28003, Security management systems for the supply chain – Requirements for bodies providing audit and certification of supply chain security management systems (Системы менеджмента безопасности для цепи поставок. Требования к органам аудита и сертификации систем менеджмента безопасности цепи поставок)

[9] ISO 28004-1, Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 – Part 1: General principles (Системы менеджмента безопасности цепи поставок. Руководящие указания по внедрению ISO 28000. Часть 1. Основные принципы)

[10] ISO 28004-3, Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 – Part 3: Additional specific guidance for adopting ISO 28000 for use by medium and small businesses (other than marine ports) (Системы менеджмента безопасности цепи поставок. Руководящие указания по внедрению ISO 28000. Часть 3. Дополнительное специальное руководство по принятию ISO 28000 для использования в операциях среднего и малого бизнеса (кроме морских портов))

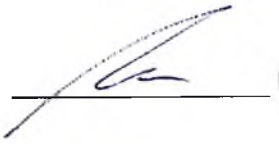
[11] ISO 28004-4, Security management systems for the supply chain – Guidelines for the implementation of ISO 28000 – Part 4: Additional specific guidance on implementing ISO 28000 if compliance with ISO 28001 is a management objective (Системы менеджмента безопасности цепи поставок. Руководящие указания по внедрению ISO 28000. Часть 4. Дополнительное специальное руководство по внедрению ISO 28000, когда соответствие ISO 28001 является предметом менеджмента)

[12] ISO 31000, Risk management – Guidelines (Менеджмент рисков. Руководство)

[13] ISO 45001, Occupational health and safety management systems – Requirements with guidance for use (Системы менеджмента здоровья и безопасности при профессиональной деятельности. Требования и руководство по применению)

[14] ISO Guide 73, Risk management – Vocabulary (Менеджмент риска. Словарь)

Заместитель директора
по техническому нормированию,
стандартизации и методологии
оценки соответствия БелГИСС  О. Ф. Ильянкова

Начальник ТО-21  И.В. Шкадрецов

Ведущий инженер ТО-21  К. Э. Маханько