

**СИСТЕМА МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК**  
Технические требования

**СІСТЭМА МЭНЭДЖМЭНТА БЯСПЕКІ ЛАНЦУГА ПАСТАВАК**  
Тэхнічныя патрабаванні

(ISO 28000:2007, IDT)

*Настоящий проект стандарта не подлежит применению до его утверждения*





### 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) ВНЕСЕН Госстандартом Республики Беларусь

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Госстандарта Республики Беларусь от №

3 Настоящий стандарт идентичен международному стандарту ISO 28000:2007 Specification for security management systems for the supply chain (Система менеджмента безопасности цепи поставок. Требования)

Международный стандарт разработан техническим комитетом по стандартизации ISO/TC8 «Судостроение и морские (морские суда) технические сооружения).

Перевод с английского языка (en).

Официальные экземпляры международного стандарта, на основе которого подготовлен настоящий государственный стандарт, и международного стандарта, на который даны ссылки, имеются в Национальном фонде ТНПА.

Степень соответствия – идентичная (IDT)

4 ВВЕДЕН ВПЕРВЫЕ

Настоящий стандарт не может быть воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Госстандарта Республики Беларусь

---

**Содержание**

Введение	IV
1 Область применения	1
2 Нормативные ссылки	1
3 Термины и определения	1
4 Элементы системы менеджмента безопасности	3
4.1 Общие требования	3
4.2 Политика в области менеджмента безопасности	3
4.3 Оценка рисков безопасности и планирование	4
4.4 Внедрение и функционирование	6
4.5 Проверка и корректирующие действия	4
4.6 Анализ со стороны руководства и постоянное улучшение	10
Приложение А (справочное) Соответствие между ISO 28000:2007, ISO 14001:2004 и ISO 9001:2000	11
Библиография	14

### Введение

Настоящий стандарт был разработан в ответ на потребность промышленности в стандарте по менеджменту безопасности. Его конечной целью является усовершенствование безопасности цепей поставок. Это стандарт менеджмента высокого уровня, позволяющий организации создать полную систему менеджмента безопасности цепей поставок. В соответствии с требованиями стандарта организация должна оценить свою рабочую среду с точки зрения обеспечения безопасности, а также определить, являются ли меры по обеспечению безопасности, принимаемые на месте, адекватными и существуют ли обязательные требования к обеспечению безопасности, которые организация должна выполнять. Если потребности в обеспечении безопасности были определены в результате этого процесса, то организация должна внедрить соответствующие механизмы и процессы, чтобы удовлетворить эти потребности. Поскольку цепи поставок по своей природе являются динамичными, некоторые организации, координирующие множество цепей поставок, могут следить за тем, чтобы их поставщики услуг выполняли соответствующие государственные стандарты по безопасности цепи поставок или соответствующие стандарты ISO, как условие включения их в цепь поставок для того, чтобы упростить менеджмент безопасности, как показано на рисунке 1.

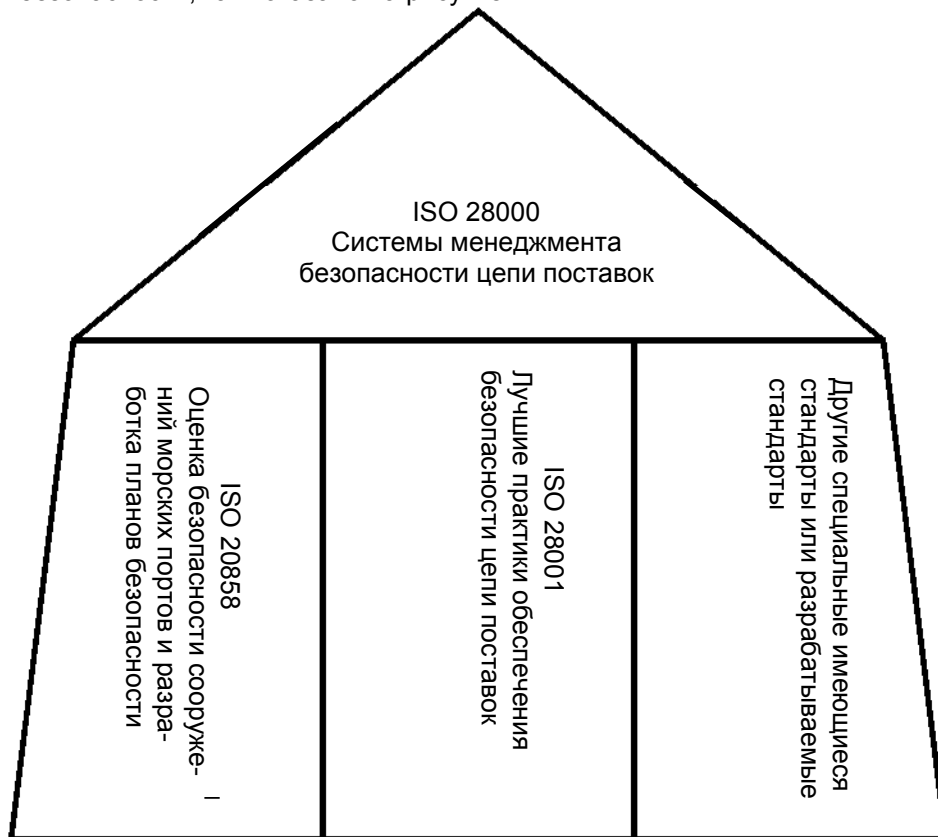


Рисунок 1 – Связь между ISO 28000 и другими соответствующими стандартами

Настоящий стандарт предназначен для применения, если цепи поставок организации требуют менеджмента безопасности. Формальный подход к менеджменту безопасности может повлиять на деловые возможности организации и доверие к ней.

Соответствие стандарту само по себе не освобождает от правовых обязательств. Для организаций, по их желанию, соответствие системы менеджмента настоящему международному стандарту может быть верифицировано путем проведения внешнего или внутреннего аудита.

Настоящий стандарт основан на ISO 14001:2004 и использует подход к системам менеджмента, основанный на анализе рисков. Однако организации, которые приняли подход к системам менеджмента, основанный на анализе процесса, (например, ISO 9001:2000), могут использовать свои существующие системы менеджмента как основу для системы менеджмента безопасности, как предписано в настоящем международном стандарте. Целью настоящего документа не является дублирование правительственных требований и стандартов, касающихся менеджмента безопасности цепи поставок, соответствие организации которым уже было сертифицировано или верифицировано. Верификация может осуществляться первой, второй или третьей стороной.

Примечание – Настоящий стандарт основывается на методологии, известной как «Plan-Do-Check-Act» (PDCA). PDCA можно описать следующим образом:

– Планирование (Plan): разработка целей и процессов, необходимых для получения результатов

в соответствии с политикой организации в области безопасности.

– Осуществление (Do): внедрение процессов.

– Проверка (Check): мониторинг и измерения процессов по отношению к политике, целям, зада-

чам, правовым и другим требованиям в области обеспечения безопасности и представление результатов.

– Действие (Act): действия по постоянному улучшению характеристик системы менеджмента

безопасности.



ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ БЕЛАРУСЬ**СИСТЕМА МЕНЕДЖМЕНТА БЕЗОПАСНОСТИ ЦЕПИ ПОСТАВОК**  
**Технические требования****СІСТЭМА МЭНЭДЖМЭНТА БЯСПЕКІ ЛАНЦУГА ПАСТАВАК**  
**Тэхнічныя патрабаванні****Specification for security management  
systems for the supply chain**

Дата введения

**1 Область применения**

Настоящий стандарт устанавливает требования к системе менеджмента безопасности, включая критические аспекты по обеспечению безопасности цепи поставок. Менеджмент безопасности связан со многими другими аспектами управления бизнесом. Аспекты включают все виды деятельности, управляемые или находящиеся под влиянием организаций, влияющие на безопасность цепи поставок. Эти аспекты должны рассматриваться непосредственно, где и когда они оказывают влияние на менеджмент безопасности, включая транспортировку этих товаров в цепи поставок.

Настоящий стандарт применим к организациям всех размеров, от небольших и до многонациональных, занимающихся изготовлением, предоставлением услуг, хранением или транспортировкой на любом этапе производства или поставок, которые хотят:

- a) разработать, внедрить, поддерживать и совершенствовать систему менеджмента безопасности;
- b) обеспечить соответствие проводимой политике в области менеджмента безопасности;
- c) продемонстрировать такое соответствие другим;
- d) добиться сертификации/регистрации системы менеджмента безопасности аккредитованным органом по сертификации; или
- e) заявить о соответствии настоящему международному стандарту.

Существуют законодательные и регулирующие нормы, отраженные в некоторых требованиях настоящего стандарта.

Настоящий стандарт не требует дублирующих доказательств соответствия.

Организации, выбирающие сертификацию третьей стороной, в дальнейшем могут продемонстрировать, что они вносят существенный вклад в безопасность цепи поставок.

**2 Нормативные ссылки**

Нормативные ссылки отсутствуют. Данный раздел включен для сохранения нумерации разделов, аналогичной нумерации других стандартов на системы менеджмента.

**3 Термины и определения**

В настоящем стандарте применены следующие термины с соответствующими определениями:

**3.1 средство** (facility): Предприятие, машины, имущество, здания, транспортные средства, суда, оборудование портов и другие объекты инфраструктуры или предприятия и связанные системы, которые выполняют определенные и количественно оцениваемые деловые функции или услуги.

Примечание – Данное определение включает системную программу, которая является необходимой для достижения безопасности и применения менеджмента безопасности.

**3.2 безопасность** (security): Противодействие намеренным несанкционированным действиям, наносящим повреждения или ущерб цепи поставок или со стороны цепи поставок.

**3.3 менеджмент безопасности (security management):** Систематические и координированные действия и инструкции, посредством которых организация оптимально управляет своими рисками и связанными возможными угрозами и воздействиями.

**3.4 цели в области менеджмента безопасности (security management objective):** Конкретные результаты или достижения, необходимые для обеспечения безопасности, для соответствия политике в области менеджмента безопасности.

Примечание – Важно, чтобы такие результаты были непосредственно или косвенно связаны с продукцией, доставкой или услугами, предоставляемыми бизнесом потребителям и конечным пользователям.

**3.5 политика в области менеджмента безопасности (security management policy):** Общие намерения и направление деятельности организации, относящиеся к обеспечению безопасности, и являющейся основой для управления процессами и действиями, связанными с обеспечением безопасности, которые установлены политикой организации и обязательными требованиями и согласуются с ними.

**3.6 программы в области менеджмента безопасности (security management programmes):** Средства, с помощью которых достигается цель в области менеджмента безопасности.

**3.7 задачи в области менеджмента безопасности (security management target):** Конкретный уровень исполнения, необходимый для достижения цели в области менеджмента безопасности.

**3.8 заинтересованное лицо (stakeholder):** Лицо или экономический субъект, имеющие законный интерес к работе, достижениям или результатам деятельности организации.

Примечание – Примеры включают потребителей, акционеров, финансистов, страховщиков, регулирующие органы, органы, предусмотренные законодательством, сотрудников, подрядчиков, поставщиков, трудовые организации или общества.

**3.9 цепь поставок (supply chain):** Связанный набор ресурсов и процессов, который начинается с получения сырья и продолжается до поставки продукции или услуг разными видами транспорта конечному потребителю.

Примечание – Цепь поставок может включать поставщиков, производственные мощности, логистов, внутренние центры распределения, дистрибьюторов, оптовиков и другие организации, связанные с конечным потребителем.

**3.9.1 последующие действия (downstream):** Относятся к действиям, процессам и перемещениям грузов в цепи поставок после того, как они выходят из-под прямого функционального управления организации, включая страхование, финансирование, менеджмент данных, а также упаковку, хранение и транспортировку грузов, но не ограничиваясь этим.

**3.9.2 предшествующие действия (upstream):** Относятся к действиям, процессам и перемещениям грузов в цепи поставок перед тем, как они попадают под прямое функциональное управление организации, включая страхование, финансирование, менеджмент данных, а также упаковку, хранение и транспортировку грузов, но не ограничиваясь этим.

**3.10 высшее руководство (top management):** Лицо или группа лиц, осуществляющих руководство и управление организацией на ее самом высоком уровне.

Примечание – Высшее руководство, особенно, крупной многонациональной организации, персонально может не заниматься деятельностью, описанной в настоящем стандарте, но реализовывать ее через свои распоряжения.

**3.11 постоянное улучшение (continual improvement):** Постоянный процесс совершенствования системы менеджмента безопасности для улучшения общих характеристик безопасности в соответствии с политикой организации в этой области.

## 4 Элементы системы менеджмента безопасности



Рисунок 2 – Элементы системы менеджмента безопасности

**4.1 Общие требования**

Организация должна разработать, документально оформить, внедрить, поддерживать и постоянно совершенствовать результативную систему менеджмента безопасности для идентификации угроз безопасности, оценки рисков, а также для контроля и уменьшения их последствий.

Организация должна постоянно повышать свою результативность в соответствии с требованиями, установленными в разделе 4.

Организация должна определить область применения своей системы менеджмента безопасности. Если организация привлекает стороннюю организацию для выполнения какого-либо процесса, влияющего на соответствие этим требованиям, то она должна обеспечить управление такими процессами. Необходимые средства управления и ответственность за процессы, выполняемые сторонней организацией, должны быть идентифицированы в системе менеджмента безопасности.

**4.2 Политика в области менеджмента безопасности**

Высшее руководство организации должно утверждать общую политику в области менеджмента безопасности. Политика должна:

- согласовываться с политикой организации в других областях;
- создавать основу, позволяющую выполнить конкретные цели, задачи и программы в области менеджмента безопасности;
- согласовываться с общей организационной структурой менеджмента угроз и рисков безопасности;
- соответствовать угрозам для организации, а также характеру и масштабу ее функционирования;
- четко определять общие/основные цели менеджмента безопасности;
- включать обязательство по постоянному совершенствованию менеджмента безопасности;
- включать обязательство по обеспечению соответствия действующему законодательству, нормативным и законодательным требованиям, а также другим требованиям, которые организация обязалась выполнять;
- быть одобрена высшим руководством;
- документально оформляться, внедряться и поддерживаться;

ж) доводится до всех вовлеченных сотрудников и третьих лиц, включая подрядчиков и посетителей, с тем, чтобы эти лица соблюдали свои обязательства, связанные с менеджментом безопасности;

к) быть доступной для заинтересованных сторон, если это необходимо;

л) предусматривать ее пересмотр, в случае приобретения других организаций или слияния с ними или других изменений в сфере деятельности организации, которые могут повлиять на непрерывность или актуальность системы менеджмента безопасности.

Примечание – Организации могут выбрать детальную политику в области менеджмента безопасности для внутреннего пользования, которая содержит достаточную информацию и указания по управлению системой менеджмента безопасности (части которой могут быть конфиденциальными), и имеет сводный (не конфиденциальный) вариант, содержащий основные цели, для распространения среди заинтересованных лиц и организаций.

### **4.3 Оценка рисков в области безопасности и планирование**

#### **4.3.1 Оценка рисков в области безопасности**

Организация должна разработать и поддерживать процедуры постоянной идентификации и оценки угроз безопасности и рисков, относящихся к менеджменту безопасности, а также идентификацию и принятие необходимых мер управления. Угрозы безопасности и идентификация рисков, методы оценки и управления, как минимум, должны соответствовать характеру и масштабу функционирования организации. Оценка должна учитывать вероятность события, и все его последствия, которая должна включать:

а) физические угрозы и риски выхода из строя, например, функциональный отказ, случайный ущерб, злоумышленное причинение вреда или террористические или преступные действия;

б) угрозы и риски, возникающие в процессе функционирования, включая управление обеспечением безопасности, человеческий фактор и другие действия, влияющие на работу, состояние и безопасность организации;

в) естественные природные явления (буря, наводнение и т. д.), которые могут привести к тому, что меры по обеспечению безопасности и сохранности оборудования окажутся неэффективными;

г) факторы, не находящиеся под управлением организации, например, дефекты оборудования и недостатки сервиса, предоставляемого внешними организациями;

д) угрозы и риски со стороны заинтересованных сторон, например, невыполнение обязательных требований или нанесение ущерба репутации или бренду;

е) конструкцию и установку оборудования по обеспечению безопасности, включая замену, техническое обслуживание и т. д.;

ж) менеджмент информации и данных, а также систему связи;

з) угрозы непрерывности функционирования.

Организация должна обеспечить, чтобы результаты этих оценок и воздействия этих средств управления рассматривались, и при необходимости, являлись входами для:

а) целей и задач менеджмента безопасности;

б) программы менеджмента безопасности;

в) определения требований к конструкции, техническим условиям и установке;

г) идентификации соответствующих ресурсов, включая численность персонала;

д) идентификации потребностей в обучении и квалификации персонала (см. 4.4.2);

е) разработки функционирования средств управления (см. 4.4.6);

ж) организационной структуры менеджмента общих угроз и рисков.

Организация должна документально оформлять и поддерживать в актуальном состоянии информацию, указанную выше.

Методология организации для идентификации и оценки угроз и рисков должна:

а) быть разработана в соответствии с областью ее применения, характером и распределением по времени, чтобы обеспечить больше предупредительный, чем реагирующий характер;

б) включать сбор информации, относящейся к угрозам и рискам безопасности;

в) предусматривать классификацию и идентификацию угроз и рисков, которые следует избегать, устранить или управлять;

г) предусматривать мониторинг действий, чтобы обеспечить эффективность и своевременность их осуществления (см. 4.5.1).

#### **4.3.2 Законодательные и другие обязательные требования, связанные с обеспечением безопасности**

Организация должна разработать, внедрить и поддерживать процедуру, чтобы:

а) идентифицировать и получить доступ к применимым правовым и другим требованиям, которые организация обязалась выполнять, относящимся к угрозам и рискам ее безопасности, и

б) определить, как эти требования распространяются на угрозы и риски для ее безопасности.

Организация должна обновлять эту информацию. Она должна передавать соответствующую информацию по правовым и другим требованиям своим сотрудникам и другим третьим лицам, которых это касается, включая подрядчиков.

#### **4.3.3 Цели в области менеджмента безопасности**

Организация должна разработать, внедрить и поддерживать документально оформленные цели для соответствующих функций и уровней в организации. Цели должны вытекать из политики организации и согласовываться с ней. При определении и пересмотре своих целей, организация должна учитывать:

а) законодательные и другие обязательные требования к обеспечению безопасности;

б) угрозы и риски, связанные с безопасностью;

с) технологические и другие возможности;

д) финансовые, функциональные и бизнес требования;

е) точку зрения соответствующих заинтересованных сторон.

Цели в области менеджмента безопасности должны:

а) соответствовать обязательствам организации по постоянному совершенствованию;

б) количественно оцениваться (если это возможно);

с) доводится всем сотрудникам и третьим лицам, которых это касается, включая подрядчиков, с целью ознакомления с их индивидуальными обязательствами;

д) периодически анализироваться, чтобы гарантировать сохранение их соответствия и согласованности с политикой в области менеджмента безопасности. В случае необходимости цели в области менеджмента безопасности должны соответственно корректироваться.

#### **4.3.4 Задачи в области менеджмента безопасности**

Организация должна разработать, внедрить и поддерживать документально оформленные задачи, соответствующие потребностям организации. Задачи должны вытекать из целей в области менеджмента безопасности и согласовываться с ними.

Указанные задачи должны:

а) быть на соответствующем уровне детализации;

б) быть конкретными, измеряемыми, решаемыми, значимыми и ограниченными во времени (если это возможно);

с) сообщаться всем сотрудникам и третьим лицам, которых это касается, включая подрядчиков, с целью ознакомления с их индивидуальными обязательствами;

д) периодически пересматриваться, чтобы гарантировать сохранение их актуальности и соответствия целям в области менеджмента безопасности. В случае необходимости в задачи должны быть внесены соответствующие изменения.

#### **4.3.5 Программы в области менеджмента безопасности**

Организация должна разработать, внедрить и поддерживать программы менеджмента безопасности для достижения своих целей и решения задач.

Программы должны быть оптимизированы, определены их приоритеты. Организация должна обеспечить эффективную и экономически результативную реализацию этих программ.

Они должны включать документацию, в которой описываются:

а) предусмотренные ответственность и полномочия для достижения целей и решения задач в области менеджмента безопасности;

б) средства и сроки, по которым цели и задачи в области менеджмента безопасности должны быть достигнуты.

Программы в области менеджмента безопасности должны периодически пересматриваться, чтобы гарантировать сохранение их результативности и соответствие целям и задачам. В случае необходимости, программы должны соответственно корректироваться.

### **4.4 Внедрение и функционирование**

#### **4.4.1 Структура, полномочия и ответственность, относящиеся к менеджменту безопасности**

Организация должна разработать и поддерживать организационную структуру ролей, ответственности и полномочий, которая согласуется с реализацией ее политики, целей, задач и программ в области менеджмента безопасности.

Роли, ответственность и полномочия должны быть определены, документально оформлены и доведены до сведения лиц, ответственных за внедрение и поддержание.

Высшее руководство должно подтвердить свои обязательства по разработке и внедрению системы (процессов) менеджмента безопасности и постоянному повышению ее результативности путем:

а) назначения члена высшего руководства, который независимо от других обязанностей должен отвечать за общую разработку, поддержание, документацию и совершенствование системы менеджмента безопасности организации;

б) назначения члена (членов) руководства с необходимыми полномочиями для обеспечения реализации целей и задач;

в) идентификации и мониторинга требований и ожиданий заинтересованных сторон и выполнения соответствующих и своевременных действий по менеджменту этих ожиданий;

г) обеспечения наличия необходимых ресурсов;

д) рассмотрения неблагоприятного влияния, которое политика, цели, задачи, программы и т. д. в области менеджмента безопасности могут оказывать на другие аспекты деятельности организации;

е) обеспечения любых программ безопасности, разработанных в других подразделениях организации, дополняющих систему менеджмента безопасности;

ж) доведения до сведения организацией важности выполнения требований к менеджменту безопасности для обеспечения соответствия своей политике;

з) обеспечения оценки и включения угроз и рисков, связанных с безопасностью, в оценку угроз и рисков организации, если это необходимо;

и) обеспечения жизнеспособности целей, задач и программ в области менеджмента безопасности.

#### 4.4.2 Компетентность, обучение и осведомленность

Организация должна обеспечить, чтобы персонал, ответственный за проектирование, функционирование и управление оборудованием и процессами, обеспечивающими безопасность, имел соответствующую квалификацию в области образования, профессиональной подготовки и/или опыт.

Организация должна разработать и поддерживать процедуры по информированию лиц, работающих в организации или от ее имени, о:

а) важности соответствия политике и процедурам в области менеджмента безопасности, а также требованиям системы менеджмента безопасности;

б) их роли и ответственности в достижении соответствия политике и процедурам в области менеджмента безопасности, а также требованиям системы менеджмента безопасности, включая требования по готовности к аварийным ситуациям и ответным действиям;

в) возможных последствиях для безопасности организации при отклонении от установленных рабочих процедур.

Записи о компетентности и обучении должны сохраняться.

#### 4.4.3 Обмен информацией

Организация должна иметь процедуры, обеспечивающие передачу необходимой информации по менеджменту безопасности соответствующим сотрудникам, подрядчикам и другим заинтересованным сторонам и получения такой информации от них.

Вследствие того, что определенная информация, связанная с безопасностью, является секретной, перед ее распространением необходимо рассмотреть степень ее конфиденциальности.

#### 4.4.4 Документация

Организация должна разработать и поддерживать документацию системы менеджмента безопасности, включающую следующие позиции, но не ограничиваясь ими:

а) политика, цели и задачи в области безопасности,

б) описание области применения системы менеджмента безопасности,

в) описание основных элементов системы менеджмента безопасности и их взаимодействия, а также ссылки на связанные документы;

г) документы, включающие записи, требуемые настоящим стандартом, и

д) документы, включающие записи, определенные организацией, необходимые для обеспечения результативного планирования, функционирования и управления процессами, связанными с существенными угрозами и рисками для ее безопасности.

Организация должна определить степень конфиденциальности информации по безопасности и предпринять шаги по предотвращению несанкционированного доступа к ней.

#### 4.4.5 Управление документацией и данными

Организация должна разработать и поддерживать процедуры управления всеми документами, данными и информацией, требуемые в разделе 4 настоящего стандарта, гарантирующие, что:

- a) эти документы, данные и информация могут размещаться только уполномоченными лицами, имеющими к ним доступ;
- b) эти документы, данные и информация периодически пересматриваются, при необходимости изменяются и подтверждаются в отношении их адекватности уполномоченным персоналом;
- c) текущие версии соответствующих документов, данные и информация доступны везде, где выполняются действия, важные для эффективного функционирования системы менеджмента безопасности;
- d) устаревшие документы, данные и информация своевременно изымаются из всех мест выдачи и мест их использования или, иначе обеспечивается их защита от непреднамеренного использования;
- e) архивные документы, данные и информация, сохраняемые для юридических целей, или в целях сохранения знаний, или для того и другого, приемлемым образом идентифицируются;
- f) эти документы, данные и информация защищены и, если они представлены в электронном виде, создаются соответствующие резервные копии, и они могут быть восстановлены.

#### 4.4.6 Функциональное управление

Организация должна идентифицировать функции и действия, необходимые для:

- a) осуществления ее политики в области менеджмента безопасности;
- b) управления деятельностью и уменьшения угроз, идентифицированных как имеющие значительный риск;
- c) соответствия законодательным и другим обязательным требованиям к обеспечению безопасности;
- d) достижения ее целей в области менеджмента безопасности;
- e) выпуска программ в области менеджмента безопасности;
- f) достижения требуемого уровня безопасности цепи поставок.

Организация должна обеспечить выполнение этих функции и действия в определенных условиях путем:

- a) установления, внедрения и поддержания документально оформленных процедур управления ситуациями, если их отсутствие может привести к невыполнению функций и действий, перечисленных выше в 4.4.6 a) – f);
- b) оценки любых угроз, создаваемых предшествующими действиями в цепи поставок, и применения средств управления для уменьшения воздействий на организацию и других последующих исполнителей цепи поставок;
- c) установления и поддержания требований к товарам или услугам, которые влияют на безопасность и информирования о них поставщиков и подрядчиков.

Эти процедуры должны включать средства управления для разработки, установки, функционирования, обновления и модификации оборудования, измерительной аппаратуры и т.д., связанных с обеспечением безопасности. Если существующие механизмы пересматриваются или вводятся новые механизмы, которые могут повлиять на функции и действия менеджмента безопасности, организация должна рассмотреть угрозы и риски для безопасности, перед их внедрением. Рассматриваемые новые или пересмотренные механизмы должны включать:

- a) пересмотренные организационную структуру, роли и ответственность;
- b) пересмотренные политику, цели, задачи или программы в области менеджмента безопасности;
- c) пересмотренные процессы и процедуры;
- d) введение новой инфраструктуры, оборудования или технологии, связанной с обеспечением безопасности, которые могут включать аппаратные средства и/или программное обеспечение;
- e) привлечение новых подрядчиков, поставщиков или персонала, если это необходимо.

#### 4.4.7 Готовность к аварийным ситуациям, реагирование и восстановление безопасности

Организация должна разработать, внедрить и поддерживать соответствующие планы и процедуры для идентификации потенциальных возможностей происшествий и аварийных ситуаций, связанных с безопасностью, ответной реакции на них, а также для предотвращения и уменьшения возможных последствий, которые могут быть с этим связаны. Планы и процедуры должны включать информацию по обеспечению и обслуживанию любого выявленного оборудования, средств или услуг, которые могут потребоваться во время происшествий или аварийных ситуаций или после них.

Организация должна периодически анализировать результативность своей готовности к аварийным ситуациям, планов и процедур реагирования и восстановления безопасности, в частности, после происшествий или аварийных ситуаций, вызываемых повреждениями в системе безопасности и угрозами. Организация должна периодически проверять эти процедуры, когда это возможно.

#### **4.5 Проверка и корректирующие действия**

##### **4.5.1 Измерения и мониторинг деятельности в области безопасности**

Организация должна разработать и поддерживать процедуры для измерения и мониторинга деятельности своей системы менеджмента безопасности. Она также должна разработать и поддерживать процедуры для мониторинга и измерения деятельности в области безопасности. Организация должна рассмотреть связанные угрозы и риски безопасности, включая возможные ухудшения механизмов и их последствия, для установления частоты проведения измерений и мониторинга ключевых параметров деятельности. Эти процедуры должны обеспечивать:

- a) как качественные, так и количественные измерения, соответствующие потребностям организации;
- b) мониторинг степени выполнения политики, целей и задач организации в области менеджмента безопасности;
- c) упреждающие критерии оценки работы, которые контролируют совместимость с программами менеджмента безопасности, критериями функционального управления и применяемыми законодательными, нормативными и другими обязательными требованиями по безопасности;
- d) реагирующие критерии оценки работы для мониторинга ухудшений, отказов, происшествий, несоответствий (включая промахи и ложные сигналы) и других предшествующих свидетельств неэффективности системы менеджмента безопасности;
- e) регистрацию данных и результатов мониторинга, достаточных для облегчения анализа корректирующих и предупредительных действий. Если для работы и/или измерений и мониторинга необходима контрольная аппаратура, организация должна потребовать введения и поддержки процедур калибровки и технического обслуживания такой аппаратуры. Записи калибровки, а также действия по техническому обслуживанию и результаты должны сохраняться в течение достаточно продолжительного промежутка времени в соответствии с законодательством и политикой организации.

##### **4.5.2 Оценивание системы**

Организация должна оценивать планы, процедуры и возможности менеджмента безопасности путем периодических анализов, испытаний, составления отчетов по происшествиям, изучения опыта, оценивания характеристик и проведения тренировок. Существенные изменения в этих факторах должны быть отражены в процедуре(ах).

Организация должна периодически оценивать соответствие деятельности законодательству и нормативным актам, лучшему промышленному опыту, а также соответствие своей собственной политике и целям.

Организация должна вести учет результатов периодических оценок.

##### **4.5.3 Отказы, происшествия, несоответствия, связанные с безопасностью, корректирующие и предупреждающие действия**

Организация должна разработать, внедрить и поддерживать процедуры для определения ответственности и полномочий, относящихся к:

- a) оцениванию и инициации предупреждающих действий по идентификации возможных отказов в системе безопасности, для возможного предотвращения;
- b) связанным с безопасностью исследованиям:
  - 1) отказов, включая промахи и ложные сигналы;
  - 2) происшествий и аварийных ситуаций;
  - 3) несоответствий;
- c) предпринимаемым действиям, для уменьшения любых последствий, возникающих в результате таких отказов, происшествий или несоответствий;
- d) инициации и завершению корректирующих действий;
- e) подтверждению результативности предпринятых корректирующих действий.

Процедуры должны требовать, чтобы все предложенные корректирующие и предупреждающие действия проверялись через процесс оценки угроз и рисков безопасности до их осуществления, если до этого не предприняты немедленные действия по предотвращению неизбежных угроз жизни или общественной безопасности.

Любые корректирующие и предупреждающие действия, предпринятые для исключения причин фактических и возможных несоответствий, должны соответствовать величине проблем и быть сораз-

мерными с угрозами и рисками для менеджмента безопасности, с которыми возможно придется столкнуться. Организация должна осуществлять и записывать любые изменения в документированных процедурах в результате корректирующих и предупреждающих действий и включить, в случае необходимости, соответствующее обучение.

#### 4.5.4 Управление записями

Организация должна разработать и поддерживать записи, необходимые для демонстрации соответствия требованиям своей системы менеджмента безопасности и настоящему стандарту, и достигнутых результатов.

Организация должна разработать, внедрить и поддерживать процедуру (процедуры) идентификации, хранения, защиты, поиска, сохранения и ликвидации записей.

Записи должны быть и оставаться разборчивыми, идентифицируемыми и прослеживаемыми.

Документация в электронном и цифровом виде должна защищаться от несанкционированного доступа, надежно резервироваться копированием и быть доступной только для уполномоченного персонала.

#### 4.5.5 Аудит

Организация должна разработать, внедрить и поддерживать программу аудита менеджмента безопасности, а также, обеспечить проведение аудитов системы менеджмента безопасности с запланированной периодичностью, чтобы:

а) определить:

1) соответствует ли система менеджмента безопасности запланированным мероприятиям по менеджменту безопасности, включая требования всего раздела 4 настоящего стандарта;

2) надлежащим ли образом эта система внедрена и поддерживается;

3) эффективна ли она в отношении соответствия политике и целям в области менеджмента безопасности.

б) анализировать результаты предыдущих аудитов и действия, предпринятые по устранению несоответствий;

с) обеспечить информацией по результатам аудитов менеджмента;

д) проверить, что оборудование и персонал, связанные с безопасностью, используются надлежащим образом.

Программа аудита, включая любой график, должна основываться на результатах оценок угроз и рисков деятельности организации, а также на результатах предыдущих аудитов. Процедуры аудитов должны охватывать область применения, частоту, методологию проведения и компетенции, а также ответственность и требования к проведению аудитов и к отчетным результатам. По возможности аудиты должны проводиться персоналом, независимым от лиц, несущих прямую ответственность за проверяемую деятельность.

Примечание - Фразу «независимый персонал» необязательно подразумевают, как персонал, не работающий в организации.

#### 4.6 Анализ со стороны руководства и постоянное улучшение

Высшее руководство должно анализировать систему менеджмента безопасности организации с запланированной периодичностью, чтобы обеспечить ее постоянную пригодность, адекватность и эффективность. Анализ должен включать оценку возможностей для улучшения и потребности в изменениях системы менеджмента безопасности, включая, политику, цели, угрозы и риски в области безопасности. Записи анализов со стороны руководства должны сохраняться. Входные данные для анализа со стороны руководства должны включать:

а) результаты аудитов и оценки соответствия законодательным и другим требованиям, которые организация обязалась выполнять,

б) обратную связь с заинтересованными сторонами, включая жалобы;

с) характеристики безопасности организации,

д) степень соответствия целям и задачам,

е) статус корректирующих и предупреждающих действий,

ф) информацию по действиям, вытекающим из предыдущего анализа со стороны руководства,

г) информацию о меняющихся обстоятельствах, включая изменения законодательных и других обязательных требований, связанных с аспектами безопасности организации, и

h) рекомендации по улучшению.

## **СТБ ISO 28000/ПР\_1**

Выходные данные анализа со стороны руководства должны включать любые решения и действия, связанные с возможными изменениями политики, целей, задач и других элементов системы менеджмента безопасности, в соответствии с обязательством постоянного улучшения.

**Приложение А**  
(справочное)

**Соответствие между ISO 28000:2007, ISO 14001:2004 и ISO 9001:2000**

Таблица А.1

ISO 28000:2007		ISO 14001:2004		ISO 9001:2000	
Элементы системы менеджмента безопасности (только заглавие)	4	Требования к системе управления окружающей средой (только заглавие)	4	Система менеджмента качества (только заглавие)	4
Общие требования	4.1	Общие требования	4.1	Общие требования	4.1
Политика в области менеджмента безопасности	4.2	Экологическая политика	4.2	Обязательства руководства Политика в области качества Постоянное улучшение	5.1 5.3 8.5.1
Оценка рисков в области безопасности и планирование (только заглавие)	4.3	Планирование (только заглавие)	4.3	Планирование (только заглавие)	5.4
Оценка рисков в области безопасности	4.3.1	Экологические аспекты	4.3.1	Ориентация на потребителя Определение требований, относящихся к продукции Анализ требований, относящихся к продукции	5.2 7.2.1 7.2.2
Законодательные и другие обязательные требования, связанные с обеспечением безопасности	4.3.2	Законодательные и другие требования	4.3.2	Ориентация на потребителя Определение требований, относящихся к продукции	5.2 7.2.1
Цели в области менеджмента безопасности	4.3.3	Целевые, плановые экологические показатели и программа(ы)	4.3.3	Цели в области качества Планирование создания и развития системы менеджмента качества Постоянное улучшение	5.4.1 5.4.2 8.5.1
Задачи в области менеджмента безопасности	4.3.4	Целевые, плановые экологические показатели и программа(ы)	4.3.3	Цели в области качества Планирование создания и развития системы менеджмента качества Постоянное улучшение	5.4.1 5.4.2 8.5.1
Программы в области менеджмента безопасности	4.3.5	Целевые, плановые экологические показатели и программа(ы)	4.3.3	Цели в области качества Планирование создания и развития системы менеджмента качества Постоянное улучшение	5.4.1 5.4.2 8.5.1
Внедрение и функционирование (только заглавие)	4.4	Внедрение и функционирование (только заглавие)	4.4	Процессы жизненного цикла продукции (только заглавие)	7
Структура, полномочия и ответственность, относящиеся к менеджменту безопасности	4.4.1	Ресурсы, обязанности, ответственность и полномочия	4.4.1	Обязательства руководства Ответственность и полномочия Представитель руководства Обеспечение ресурсами Инфраструктура	5.1 5.5.1 5.5.2 6.1 6.3
Компетентность, обучение и осведомленность	4.4.2	Компетентность, обучение и осведомленность	4.4.2	(Человеческие ресурсы) Общие положения Компетентность, осведомленность и подготовка	6.2.1 6.2.2

СТБ ISO 28000/ПР\_1

Продолжение таблицы А.1

ISO 28000:2007		ISO 14001:2004		ISO 9001:2000	
Обмен информацией	4.4.3	Обмен информацией	4.4.3	Внутренний обмен информацией Связь с потребителями	5.5.3 7.2.3
Документация	4.4.4	Документация	4.4.4	(Требования к документации) Общие положения	4.2.1
Управление документацией и данными	4.4.5	Управление документацией	4.4.5	Управление документацией	4.2.3
Функциональное управление	4.4.6	Управление операциями	4.4.6	Планирование процессов жизненного цикла продукции	7.1
				Определение требований, относящихся к продукции	7.2.1
				Анализ требований, относящихся к продукции	7.2.2
				Планирование проектирования и разработки	7.3.1
				Входные данные для проектирования и разработки	7.3.2
				Выходные данные проектирования и разработки	7.3.3
				Анализ проекта и разработки	7.3.4
				Верификация проекта и разработки	7.3.5
				Валидация проекта и разработки	7.3.6
				Управление изменениями проекта и разработки	7.3.7
				Процесс закупок	7.4.1
				Информация по закупкам	7.4.2
Верификация закупленной продукции	7.4.3				
Управление производством и обслуживанием	7.5.1				
Валидация процессов производства и обслуживания	7.5.2				
Сохранение соответствия продукции	7.5.5				
Готовность к аварийным ситуациям, реагирование и восстановление безопасности	4.4.7	Готовность к аварийным ситуациям и реагирование на них	4.4.7	Управление несоответствующей продукцией	8.3
Проверка и корректирующие действия (только заглавие)	4.5	Проверка (только заглавие)	4.5	Измерение, анализ и улучшения (только заглавие)	8
Измерение и мониторинг деятельности в области безопасности	4.5.1	Мониторинг и измерение	4.5.1	Управление устройствами для мониторинга и измерений	7.6
				Общие положения (Измерение, анализ и улучшение)	8.1
				Мониторинг и измерение процессов	8.2.3
				Мониторинг и измерение продукции	8.2.4
				Анализ данных	8.4

Окончание таблицы А.1

ISO 28000:2007		ISO 14001:2004		ISO 9001:2000	
Оценивание системы	4.5.2	Оценка соответствия	4.5.2	Мониторинг и измерение процессов Мониторинг и измерение продукции	8.2.3 8.2.4
Отказы, происшествия, несоответствия, связанные с безопасностью, корректирующие и предупреждающие действия	4.5.3	Несоответствие, корректирующие и предупреждающие действия	4.5.3	Управление несоответствующей продукцией Анализ данных Корректирующие действия Предупреждающие действия	8.3 8.4 8.5.2 8.5.3
Управление записями	4.5.4	Управление записями	4.5.4	Управление записями	4.2.4
Аудит	4.5.5	Внутренний аудит	4.5.5	Внутренние аудиты (проверки)	8.2.2
Анализ со стороны руководства и постоянное улучшение	4.6	Анализ со стороны руководства	4.6	Обязательства руководства Анализ со стороны руководства (только заглавие) Общие положения Входные данные для анализа Выходные данные анализа Постоянное улучшение	5.1 5.6 5.6.1 5.6.2 5.6.3 8.5.1

**Библиография**

- [1] ISO 9001:2000 Quality management systems. Requirements  
(Системы менеджмента качества. Требования)
- [2] ISO 14001:2004 Environmental management systems. Requirements with guidance for use  
(Системы управления окружающей средой. Требования и руководство по применению)
- [3] ISO 19011:2002 Guidelines for quality and/or environmental management systems auditing  
(Руководящие указания по аудиту систем менеджмента качества и/или систем экологического менеджмента)
- [4] ISO/PAS 20858:2004 Ships and marine technology. Maritime port facility security assessments and security plan development  
(Суда и морские технологии. Оценка безопасности сооружений морских портов и разработка планов безопасности)
- [5] ISO/PAS 28001 Security management systems for the supply chain. Best practices for implementing supply chain security. Assessments and plans  
(Системы менеджмента безопасности цепи поставок. Практическое руководство по обеспечению безопасности цепи поставок. Оценка и планы)
- [6] ISO/PAS 28004:2006 Security management systems for the supply chain — Guidelines for the implementation of ISO/PAS 28000  
(Системы управления безопасностью для цепи поставок. Руководство по применению стандарта ISO/PAS 28000)

Директор БелГИСС	_____	В. Л. Гуревич
Заместитель директора БелГИСС по подтверждению соответствия	_____	И. И. Осмола
Начальник ТО-21	_____	О. М. Самсоненко
Начальник ТС-211	_____	И. В. Шкадрецов
Техник ТО-21	_____	Т. М. Шлык