МЕЖГОСУДАРСТВЕННЫЙ СОВЕТ ПО СТАНДАРТИЗАЦИИ, МЕТРОЛОГИИ И СЕРТИФИКАЦИИ
(МГС)
INTERSTATE COUNCIL FOR STANDARDIZATION, METROLOGY AND CERTIFICATION
(ISC)

МЕЖГОСУДАРСТВЕННЫЙ СТАНДАРТ

ГОСТ ISO/IEC 27014— 2021

Информационные технологии

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, КИБЕРБЕЗОПАСНОСТЬ И ЗАЩИТА КОНФИДЕНЦИАЛЬНОСТИ

Руководство деятельностью по обеспечению информационной безопасности

(ISO/IEC 27014:2020, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

Цели, основные принципы и общие правила проведения работ по межгосударственной стандартизации установлены ГОСТ 1.0 «Межгосударственная система стандартизации. Основные положения» и ГОСТ 1.2 «Межгосударственная система стандартизации. Стандарты межгосударственные, правила и рекомендации по межгосударственной стандартизации. Правила разработки, принятия, обновления и отмены»

Сведения о стандарте

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН), Обществом с ограниченной ответственностью «Информационно-аналитический центр» (ООО ИАВЦ) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 5

2 ВНЕСЕН Межгосударственным техническим комитетом по стандартизации МТК 022 «Информационные технологии»

3 ПРИНЯТ Межгосударственным советом по стандартизации, метрологии и сертификации (протокол от 30 июня 2021 г. № 141-П)

За принятие проголосовали:

Краткое наименование страны по МК (ИСО 3166) 004—97	Код страны по МК (ИСО 3166) 004—97	Сокращенное наименование национального органа по стандартизации
Армения	AM	ЗАО «Национальный орган по стандартизации и метрологии» Республики Армения
Беларусь	BY	Госстандарт Республики Беларусь
Киргизия	KG	Кыргызстандарт
Россия	RU	Росстандарт
Узбекистан	UZ	Узстандарт

4 Приказом Федерального агентства по техническому регулированию и метрологии от 2 июля 2021 г. № 613-ст межгосударственный стандарт ГОСТ ISO/IEC 27014—2021 введен в действие в качестве национального стандарта Российской Федерации с 30 ноября 2021 г.

5 Настоящий стандарт идентичен международному стандарту ISO/IEC 27014:2020 «Информационные технологии. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство деятельностью по обеспечению информационной безопасности» («Information technology — Information security, cybersecurity and privacy protection— Governance of information security», IDT).

ISO/IEC 27014:2020 разработан подкомитетом SC 27 «Информационная безопасность, кибербезопасность и защита конфиденциальности» Совместного технического комитета JTC 1 «Информационные технологии» Международной организации по стандартизации (ISO) и Международной электротехнической комиссии (IEC).

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им межгосударственные стандарты, сведения о которых приведены в дополнительном приложении ДА

6 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории указанных выше государств публикуется в указателях национальных стандартов, издаваемых в этих государствах, а также в сети Интернет на сайтах соответствующих национальных органов по стандартизации.

В случае пересмотра, изменения или отмены настоящего стандарта соответствующая информация будет опубликована на официальном интернет-сайте Межгосударственного совета по стандартизации, метрологии и сертификации в каталоге «Межгосударственные стандарты»

Содержание

Введение

Обеспечение информационной безопасности (ИБ) является важнейшей задачей организаций, значение которой постоянно повышается в результате непрерывного развития методов и средств проведения атак на информационные системы, а также в связи с усилением нормативных требований регуляторов.

Недостаточность мер обеспечения ИБ может иметь как для организации, так и для ее партнеров множество негативных последствий, в том числе связанных с утратой доверия.

Руководство деятельностью по обеспечению ИБ предполагает надлежащее использование ресурсов для обеспечения эффективной реализации ИБ, обеспечивающей уверенность в том, что:

- будут соблюдаться директивы по ИБ;
- руководство будет получать достоверную и актуальную отчетность о деятельности, связанной с ИБ.

Предоставленная информация об ИБ помогает руководству принимать решения относительно стратегических целей организации, что гарантирует кроме прочего и соответствие стратегии ИБ этим целям. Она также обеспечивает соответствие стратегии информационной безопасности общим целям организации.

Менеджеры и другие работники организации должны понимать следующее:

- требования к руководству деятельностью, влияющие на их работу;
- как удовлетворить требования к руководству деятельностью, требующие их действий.

Поправка к ГОСТ ISO/IEC 27014—2021 Информационные технологии. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство деятельностью по обеспечению информационной безопасности

Дата введения — 03.09.2021

В каком месте	Напечатано	Должно быть		
Предисловие. Таблица согласования	—	Казахстан	KZ	Госстандарт Республики Казахстан

(ИУС № 11 2021 г.)

М Е Ж Г О С У Д А Р С Т В Е Н Н Ы Й С Т А Н Д А Р Т

Информационные технологии

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, КИБЕРБЕЗОПАСНОСТЬ И ЗАЩИТА КОНФИДЕНЦИАЛЬНОСТИ

Руководство деятельностью по обеспечению информационной безопасности

Information technology. Information security, cybersecurity and privacy protection. Governance of information security

Дата введения — 2021—11—30

1 Область применения

В настоящем стандарте представлены понятия, цели и процессы руководства деятельностью по обеспечению информационной безопасности (ИБ), с помощью которых организации могут оценивать, направлять, контролировать и передавать информацию о процессах, связанных с ИБ, внутри организации.

Целевая аудитория настоящего стандарта:

- руководящие органы и лица из состава высшего руководства;
- лица, ответственные за оценку, управление и мониторинг системы менеджмента информационной безопасности (СМИБ) на основе ISO/IEC 27001;
- лица, ответственные за менеджмент ИБ за пределами области действия СМИБ, основанной на ISO/IEC 27001, но в рамках руководства деятельностью.

Настоящий стандарт применим ко всем видам организаций с различной численностью работников (персонала).

Все ссылки на СМИБ в настоящем стандарте относятся к СМИБ, соответствующим ISO/IEC 27001.

В настоящем стандарте основное внимание уделяется организациям трех типов по отношению к СМИБ, приведенным в приложении В. Однако настоящий стандарт может также использоваться и для организаций других типов.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты. Для датированных ссылок применяют только указанное издание ссылочного стандарта, для недатированных — последнее издание (включая все изменения).

ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary (Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология)

ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements **(**Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования)

Издание официальное

3 Термины и определения

В настоящем стандарте применены термины по ISO/IEC 27000, а также следующие термины с соответствующими определениями:

ISO и IEC поддерживают терминологические базы, используемые в сфере стандартизации, доступные на следующих сайтах:

- Онлайн-библиотека стандартов ISO: https://www.iso.org/obp;
- IEC Electropedia: https://www.electropedia.org/;
- термины и определения ITU-T: http://www.itu.int/go/terminology-databasehttp://www.itu.int/go/terminology-databasehttp://www.itu.int/go/terminology-database.

3.1 **организационная структура** (entity): Предприятие, учреждение или другой хозяйствующий субъект.

Примечание — Организационная структура может быть группой компаний, отдельной компанией, некоммерческой организацией или чем-нибудь иным. Организационная структура имеет руководящие полномочия над организацией. В отдельных случаях, например, в небольших компаниях организационная структура может быть идентична организации.

3.2 **организация** (organization): Часть организационной структуры, в которой эксплуатируется и контролируется система менеджмента информационной безопасности (СМИБ).

3.3 **руководящий орган** (governing body): Лицо или группа лиц, несущих ответственность за производительность организационной структуры (3.1) и за соблюдение применимых ею норм.

[ISO/IEC 27000:2018 (подраздел 3.24) с изменениями — вместо термина «организация» используется термин «организационная структура»]

3.4 **высшее руководство** (top management): Лицо или группа лиц, руководящих организацией (3.2) и контролирующих ее на высшем уровне.

Примечания

1 Высшее руководство имеет право делегировать полномочия и предоставлять ресурсы в рамках организации.

2 Если область действия системы менеджмента охватывает только часть организационной структуры, то высшее руководство относится к тем, кто руководит этой частью организационной структуры и контролирует ее. Высшее руководство подотчетно руководящему органу организационной структуры.

3 В зависимости от размера и ресурсов организации, высшее руководство может быть совмещено с руководящим органом.

4 Высшее руководство подчиняется руководящему органу.

5 В ISO 37001 также определены понятия руководящего органа и высшего руководства.

[ISO/IEC 27000:2018 (подраздел 3.75) с изменениями:

- в примечании 2 термин «организация» заменен на термин «организационная структура» и добавлено второе предложение;
- примечание 3 заменено;
- добавлены примечания 3 и 5]

4 Сокращения

В настоящем стандарте применены следующие сокращения:

СМИБ — система менеджмента информационной безопасности;

ИТ — информационные технологии.

5 Состав и структура настоящего стандарта

В настоящем стандарте описано, как осуществляется руководство деятельностью по обеспечению ИБ в рамках СМИБ, соответствующей ISO/IEC 27001, и как такие руководящие действия могут быть связаны с другими действиями управления вне области действия СМИБ. В настоящем стандарте определены четыре основных процесса: «оценка», «координация», «мониторинг» и «обмен информацией», в которых СМИБ может быть структурирована внутри организации, а также предлагаются подходы для интеграции руководства деятельностью по обеспечению ИБ в деятельность по управлению организацией для каждого из этих процессов. В приложении А описываются взаимосвязи между управлением

организацией, управлением информационными технологиями и управлением деятельностью по обеспечению ИБ.

По определению организация охватывает всю организационную структуру (см. ISO/IEC 27000). Но она может охватывать как всю организационную структуру, так и его часть, как показано на рисунке В.1.

6 Руководство деятельностью и стандарты управления

6.1 Обзор

Руководство деятельностью по обеспечению ИБ — это процесс, посредством которого руководящий орган организации обеспечивает общую координацию и контроль деятельности, связанной с ИБ. Координация и контроль фокусируются на ситуациях, когда недостатки в обеспечении информационной безопасности могут негативно влиять на способность организации достигать своих основных целей. Руководящий орган обычно реализует цели своего управления деятельностью посредством:

- обеспечения координации путем определения стратегий и политик;
- мониторинга деятельности организации;
- оценки предложений и планов, разработанных руководителями.

Управление ИБ связано с обеспечением достижения целей организации, описанных в стратегиях и политиках, определенных руководящим органом. Кроме того, взаимодействие с руководящим органом может включать в себя:

- представление на рассмотрение руководящего органа предложений и планов;
- предоставление руководящему органу информации о деятельности организации.

Эффективное руководство деятельностью по обеспечению ИБ требует, чтобы как члены руководящего органа, так и менеджеры надлежащим образом выполняли соответствующие обязанности.

6.2 Руководство деятельностью в рамках системы менеджмента информационной безопасности

ISO/IEC 27001 определяет требования к созданию, внедрению, поддержке и постоянному улучшению СМИБ в контексте организации. Он также включает требования к оценке и обработке рисков ИБ с учетом потребностей организационной структуры.

В ISO/IEC 27001 не используется термин «руководство деятельностью», но в нем определен ряд требований, удовлетворение которых обеспечивается действиями управления. Далее приведены примеры таких действий. Как уже отмечалось ранее, понятия «организация» и «высшее руководство» относятся к области действия СМИБ на основе ISO/IEC 27001:

- ISO/IEC 27001:2013, 4.1, требует, чтобы организация идентифицировала то, чего она стремится достичь, — цели и задачи своей ИБ. Они должны быть связаны с общими целями и задачами организационной структуры и поддерживать их. Это относится к целям руководства деятельностью, определенным в 7.2.1, 7.2.3 и 7.2.4 настоящего стандарта;
- ISO/IEC 27001:2013, 4.2, требует, чтобы организация идентифицировала заинтересованные стороны, имеющие отношение к ее СМИБ, а также требования этих заинтересованных сторон, относящиеся к ИБ. Это относится к цели руководства деятельностью, определенной в 7.2.4 настоящего стандарта;
- ISO/IEC 27001:2013, 4.3, требует, чтобы организация определила границы и применимость СМИБ для установления ее области применения с учетом внешних и внутренних факторов, требований, интерфейсов и зависимостей. Кроме того, в своей СМИБ организация должна удовлетворять требованиям и ожиданиям заинтересованных сторон, а также учитывать внешние и внутренние факторы, такие как законы, нормативные акты и контракты. Это относится к цели руководства деятельностью, определенной в 7.2.1 настоящего стандарта;
- ISO/IEC 27001:2013, раздел 5, определяет, что организация должна установить политику и цели, а также интегрировать ИБ в свои процессы (которые можно рассматривать как включающие в себя процессы руководства деятельностью). Это потребует от организации предоставления надлежащих ресурсов и информирования о важности управления информационной безопасностью. Очень важно, что в этом разделе также указано, что организация должна направлять и стимулировать людей, чтобы они вносили свой вклад в эффективность СМИБ, а также должна поддерживать другие соответствующие роли менеджмента в их областях ответственности. ISO/IEC 27001:2013, раздел 5, содержит инструкции по настройке политики и назначению ролей для менеджмента информационной безопасности и отчет-

ности. Это относится к целям руководства деятельностью, определенным в 7.2.1 и 7.2.3 настоящего стандарта;

- ISO/IEC 27001:2013, раздел 6, рассматривает разработку подхода к менеджменту рисков для организации, указывая, что организация должна идентифицировать риски и возможности, которые необходимо учитывать, чтобы гарантировать эффективность ее СМИБ. Он вводит понятие владельцев рисков и помещает их обязанности в контекст деятельности организации по управлению рисками и утверждению действий по обработке рисков. При этом также требуется, чтобы организация установила цели информационной безопасности. Это относится к цели руководства деятельностью, определенной в 7.2.2 настоящего стандарта;

- ISO/IEC 27001:2013, раздел 7, представляет требования к коммуникациям организации и определяет, что в выполнении своих обязательств по ИБ сотрудники должны иметь соответствующий уровень компетентности. Это относится к цели руководства деятельностью, определенной в 7.2.5 настоящего стандарта;

- ISO/IEC 27001:2013, раздел 8, требует, чтобы организационная структура планировала, внедряла и контролировала свою СМИБ, даже если она передана в аутсорсинг. Это относится к целям руководства деятельностью, определенным в 7.2.4 и 7.2.6 настоящего стандарта;

- ISO/IEC 27001:2013, раздел 9, требует мониторинга и отчетности по всем соответствующим аспектам СМИБ, внутреннего аудита, а также анализа и решений высшего руководства и руководящего органа по операционной эффективности СМИБ, включая любые требуемые изменения. Это относится к цели руководства деятельностью, определенной в 7.2.6 настоящего стандарта;

- ISO/IEC 27001:2013, раздел 10, определяет идентификацию и обработку несоответствий, требование определения возможностей для постоянного улучшения, а также действий в соответствии с этими возможностями. Это относится к цели руководства деятельностью, определенной в 7.2.4 настоящего стандарта.

6.3 Другие стандарты, связанные с руководством деятельностью

ISO/IEC 38500 определяет принципы для руководящих органов организаций по надлежащему, действенному и эффективному использованию информационных технологий в организациях. В нем также содержатся рекомендации для тех, кто консультирует, информирует или помогает руководящим органам в управлении ИТ.

6.4 Направления руководства деятельностью организации

Направления руководства деятельностью организации полностью соответствуют процессам управления организацией, описанным в разделе 7. Последние два элемента в списке являются эквивалентами их аспектов управления в контексте ИБ:

- согласование целей ИБ с бизнес-целями;
- управление рисками ИБ в соответствии с целями ИБ;
- избежание конфликта интересов при управлении ИБ;
- предотвращение использования ИТ организации во вред другим организационным структурам.

7 Руководство деятельностью организационной структуры и руководство деятельностью по обеспечению информационной безопасности

7.1 Общие положения

В рамках организационной структуры существует ряд направлений руководства деятельностью, включая ИБ, ИТ, здоровье и безопасность, качество и финансы. Каждое направление области руководства деятельностью является составной частью задачи достижения общих целей корпоративного управления и поэтому должно соответствовать установленной практике организационной структуры. Рамки моделей руководства деятельностью в некоторых случаях пересекаются. В 7.2 и 7.3 описываются цели и процессы, присущие руководству деятельностью по обеспечению ИБ, применимые для любой области руководства деятельностью.

СМИБ ориентирована на управление рисками, связанными с информацией. Она не касается напрямую таких вопросов, как прибыльность, приобретение, использование и реализация активов или

эффективность других процессов, но она должна поддерживать любые организационные цели, связанные с этими аспектами.

7.2 Цели

7.2.1 Цель 1: Обеспечение всеобъемлющей интегрированной информационной безопасности на уровне организационной структуры

Руководство деятельностью по обеспечению ИБ должно гарантировать, что цели ИБ являются всеобъемлющими и интегрированными. Информационной безопасностью следует заниматься на уровне организационной структуры, с принятием решений с учетом приоритетов организационной структуры. Действия, касающиеся физической и логической безопасности, должны быть тщательно скоординированы. Но при этом не обязательно иметь одну совокупность мер обеспечения безопасности или единую СМИБ для всей организационной структуры.

В целях обеспечения ИБ в масштабах всей организационной структуры для всего диапазона ее деятельности должны быть установлены ответственность за ИБ и соответствующая подотчетность. Область ИБ может выходить за пределы обычно воспринимаемых «границ» организационной структуры, например включать информацию, хранящуюся или передаваемую внешними сторонами.

7.2.2 Цель 2: Принятие решений на основе оценки рисков

Руководство деятельностью по обеспечению ИБ должно основываться на обязательствах по соблюдению требований, а также на решениях, основанных на оценке специфичных для организационной структуры рисков. Определение приемлемой степени безопасности должно основываться на допустимых для организационной структуры уровнях рисков, включая риски потери конкурентного преимущества, риски несоответствия и невыполнения обязательств, риски сбоев в работе, риски репутационного ущерба и финансовых убытков.

Управление рисками ИБ должно быть единообразным для всей организационной структуры и включать в себя анализ неблагоприятных финансовых, операционных и репутационных последствий нарушений и несоблюдения требований. Кроме того, управление рисками ИБ должно быть интегрировано с общим подходом к управлению рисками организационной структуры, чтобы оно не выполнялось изолированно и не вызывало путаницы, например, при сопоставлении с методологией организации или при записи стратегических информационных рисков в реестр рисков организации.

Для реализации управления информационными рисками соответствующие ресурсы должны быть выделены как часть процесса управления безопасностью.

7.2.3 Цель 3: Обеспечение координации приобретений

При проведении новых мероприятий, таких как любые инвестиции, покупки, слияние, внедрение новых технологий, заключения соглашений об аутсорсинге и контрактов с внешними поставщиками, необходимо должным образом оценить воздействия рисков ИБ.

Для оптимизации ИБ для поддержки целей организационной структуры руководящий орган должен обеспечить интеграцию информационной безопасности с существующими процессами организационной структуры, включая управление проектами, закупками, финансовыми расходами, соответствием законодательным и нормативным требованиям и управление стратегическими рисками.

Для каждой СМИБ высшее руководство должно разработать стратегию ИБ, основанную на целях организационной структуры, обеспечивая гармонизацию между требованиями организационной структуры и требованиями ИБ организации, удовлетворяя таким образом текущие и будущие потребности заинтересованных сторон.

7.2.4 Цель 4: Обеспечение соответствия внутренним и внешним требованиям

Руководство деятельностью по обеспечению ИБ должно гарантировать соответствие политик и практики ИБ требованиям заинтересованных сторон, которые могут включать в себя законы, нормативные акты, а также договорные требования и внутренние обязательства.

Для обеспечения уверенности в том, что деятельность по ИБ должным образом соответствует внутренним и внешним требованиям соответствия, а также для подтверждения этого соответствия высшее руководство может заказать независимый аудит безопасности.

7.2.5 Цель 5: Развитие культуры безопасности

Руководство деятельностью по обеспечению ИБ должно основываться на культурных ценностях организационной структуры с учетом меняющихся потребностей всех заинтересованных сторон, поскольку человеческое поведение является одним из фундаментальных элементов, обеспечивающих соответствующий уровень ИБ. Если не координировать цели, роли, обязанности и ресурсы должным

образом, то они могут противоречить друг другу, что приведет к неспособности достичь каких-либо целей. Поэтому гармонизация и согласованная ориентация различных заинтересованных сторон очень важны.

В целях создания позитивной культуры ИБ высшее руководство должно требовать, поощрять и поддерживать координацию действий заинтересованных сторон для достижения последовательной координации ИБ. Этому способствует реализация образовательных, обучающих и информационных программ по вопросам безопасности. Обязанности по ИБ должны быть интегрированы в роли персонала и других сторон, которые, принимая на себя эти обязанности, и должны обеспечивать эффективность любой СМИБ.

7.2.6 Цель 6: Обеспечение соответствия показателей безопасности текущим и будущим требованиям организационной структуры

Руководство деятельностью по обеспечению ИБ должно гарантировать, что выбранный подход к защите информации соответствует цели поддержки организационной структуры, обеспечивая согласованные уровни ИБ. Показатели безопасности следует контролировать и поддерживать на уровне, необходимом для удовлетворения текущих и будущих требований.

Чтобы проанализировать эффективность ИБ с точки зрения руководства деятельностью, руководящий орган должен оценить не только результативность и действенность мер безопасности, но и на уровне организационной структуры оценить эффективность ИБ по отношению к ее влиянию.

В рамках каждой СМИБ от высшего руководства следует требовать внедрения программы оценки эффективности для мониторинга, аудита и выявления возможностей для улучшения. Руководящему органу следует увязать эффективность информационной безопасности с производительностью организации и организационной структуры в целом.

7.3 Процессы

7.3.1 Общие положения

Действия руководящего органа в организационной структуре реализуются выполнением процессов: «оценка», «координация», «мониторинг» и «обмен информацией». На рисунке 1 показана взаимосвязь между этими процессами.

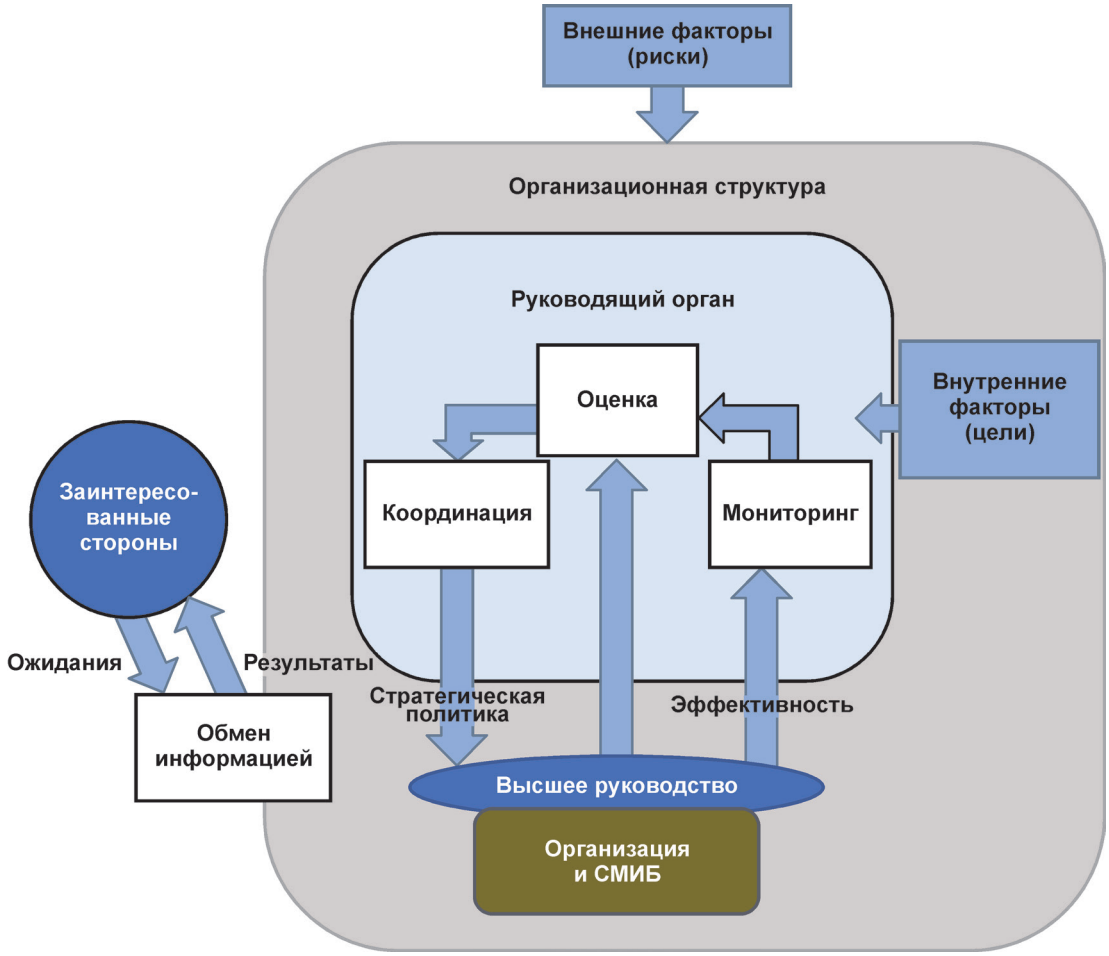


Рисунок 1 — Модель управления организационной структурой с одной системой менеджмента информационной безопасности

Примечания

1 Определение организации (3.2) подразумевает, что высшее руководство всегда полностью вовлечено в работу организации.

2 В состав организационной структуры может входить более одной СМИБ, но могут быть и такие части организационной структуры, к которым применимо руководство деятельностью, но которые не охвачены СМИБ (см. раздел 8 и приложение В).

7.3.2 Оценка

«Оценка» представляет собой процесс руководства деятельностью, в ходе которого анализируется текущее и прогнозируемое достижение целей на основе текущих процессов и запланированных изменений и определяется, где требуются какие-либо корректировки для оптимизации достижения стратегических целей в будущем.

В процессе «оценка» руководящий орган организационной структуры должен:

- гарантировать, что инициативы учитывают соответствующие риски и возможности;
- реагировать на оценки ИБ, СМИБ и соответствующие отчеты путем определения целей и их приоритетов в контексте каждой СМИБ, что также включает и рассмотрение требований вне области действия СМИБ.

В процессе «оценка» высшее руководство каждой СМИБ должно:

- гарантировать, что ИБ должным образом поддерживает цели организационной структуры и способствует их достижению;
- представлять на одобрение руководящему органу новые значимые проекты ИБ.

7.3.3 Координация

«Координация» — это процесс руководства деятельностью, посредством которого руководящий орган задает направления развития целей и стратегии организационной структуры. Координация может включать в себя изменения в уровнях обеспечения ресурсами, изменения распределения ресурсов и приоритетов деятельности, утверждение политик, принятие существенных рисков и планов управления рисками.

В процессе «координация» руководящий орган должен:

- определить общее стратегическое направление и цели организационной структуры;
- определить уровень предпочтительного риска организационной структуры;
- утвердить стратегию безопасности информации.

В процессе «координация» высшее руководство каждой СМИБ должно:

- выделить соответствующие инвестиции и ресурсы;
- согласовать цели ИБ организационной структуры с целями организационной структуры;
- распределить роли и обязанности по ИБ;
- установить политику ИБ.

Примечание — Предпочтительный риск — это тип риска и его уровень, к которому организация стремится или готова поддерживать.

7.3.4 Мониторинг

«Мониторинг» является процессом управления деятельностью, позволяющим руководству контролировать ее текущее состояние, оценивать достижение стратегических целей.

Мониторинг — это система постоянного наблюдения за явлениями и процессами, проходящими в окружающей среде и обществе, результаты которого служат для обоснования управленческих решений по обеспечению безопасности людей и объектов.

В процессе «мониторинг» руководящий орган должен:

- получать отчет об эффективности работы каждой СМИБ;
- оценивать отчеты с точки зрения приоритетов организационной структуры;
- докладывать о приоритетах высшему руководству каждой СМИБ.

В процессе «мониторинг» высшее руководство каждой СМИБ должно:

- оценивать эффективность деятельности по управлению ИБ;
- обеспечить соответствие внутренним и внешним требованиям;
- учитывать изменяющуюся структуру, правовую и нормативную среду, а также любое потенциальное влияние на информационные риски;
- выбрать подходящие показатели эффективности и требовать своевременной отчетности с организационной точки зрения;
- обеспечивать руководящему органу обратную связь о результатах деятельности по обеспечению ИБ;
- предупреждать руководящий орган о новых событиях, влияющих на информационные риски и ИБ.

Чтобы проанализировать эффективность ИБ с точки зрения руководства деятельностью, высшее руководство должно оценивать не только результативность и действенность средств обеспечения безопасности, но и эффективность ИБ относительно ее воздействия на уровне организационной структуры и подразделений. Анализ может быть выполнен путем реализации программы оценки производительности для мониторинга, аудита и выявления возможностей улучшения путем сопоставления эффективности ИБ с производительностью организации и организационной структуры в целом.

7.3.5 Обмен информацией

«Обмен информацией» представляет собой двусторонний процесс руководства деятельностью, при котором руководящий орган и заинтересованные стороны обмениваются данными, соответствующими их конкретным потребностям.

Одним из возможных документов «обмена информацией» может быть отчет о состоянии ИБ, в котором заинтересованным сторонам разъясняются действия и проблемы ИБ.

Одной из причин обмена информацией является необходимость обеспечить должную ответственность организационной структуры перед заинтересованными сторонами, такими как акционеры. Обмен информацией становится все более важным, и организационные структуры предоставляют информацию о реализации и поддержке своих СМИБ, а также об эффективности управления рисками. Кроме того, в случае если произошел инцидент ИБ, организационная структура должна объяснить влияние,

причины и изменения в мерах обеспечения безопасности для снижения риска повторных инцидентов всем своим заинтересованным сторонам, а при необходимости — дополнительно — и широкой общественности.

Обмен информацией может осуществляться разными способами. Он также может быть различным по содержанию и иметь самые разные аудитории. Любой обмен информацией должен быть спроектирован с учетом аудитории, а также сообщений, которые, как предполагается, аудитория должна понимать. Эти два фактора следует использовать для определения содержания сообщений, а также каналов, используемых для доставки сообщений целевой аудитории. Один из примеров приведен в приложении С.

В процессе «обмен информацией» руководящий орган должен:

- сообщать внешним заинтересованным сторонам о том, что организационная структура обеспечивает уровень ИБ, соответствующий характеру ее деятельности и приоритетам;
- специфицировать и определять приоритеты нормативных обязательств, ожиданий заинтересованных сторон и требований организационной структуры в отношении ИБ;
- консультировать высшее руководство каждой СМИБ по любым вопросам, требующим его внимания и решения;
- подробно инструктировать соответствующие заинтересованные стороны о целях, которых необходимо достигнуть в поддержку приоритетов ИБ;
- развивать культуру ИБ;
- обучать обязанностям и обсуждать их с персоналом и другими лицами, имеющими отношение к СМИБ.

8 Требования руководящего органа к системе менеджмента информационной безопасности

8.1 Организация и система менеджмента информационной безопасности

Для поддержки целей организационной структуры руководящий орган должен требовать разработки одной или нескольких СМИБ. Цели каждой СМИБ могут либо совпадать с целями самой организационной структуры либо, в зависимости от размера, масштаба и структуры всей организационной структуры, могут отличаться от целей организационной структуры, но должны быть согласованы с ними. Возможные связи между руководством деятельностью по обеспечению ИБ и руководством деятельностью ИТ показаны в приложении А.

Руководящий орган должен также требовать, чтобы проект каждой СМИБ соответствовал общим политикам и процессам организационной структуры, включая управление рисками. Для обеспечения четкого обмена информацией о рисках может оказаться целесообразным использовать в СМИБ тот же процесс оценки рисков, который применяется руководящим органом.

Руководящий орган должен также требовать, чтобы проект каждой СМИБ соответствовал общим политикам и процессам организационной структуры, включая управление рисками. Для обеспечения четкого обмена информацией о рисках представляется целесообразным использовать в СМИБ процесс оценки рисков, принятый руководящим органом. Однако если данный процесс не соответствует требованиям ISO/IEC 27001, подход к оценке рисков оператора СМИБ, принятый в целях соответствия с этим стандартом, будет отличаться от принятого для организации в целом. В таком случае должен быть предложен метод передачи информации о рисках в виде, совместимом с подходом руководящего органа. В качестве альтернативы руководящий орган может изменить существующий процесс оценки рисков организационной структуры, с тем чтобы он соответствовал требованиям ISO/IEC 27001.

Руководящий орган может санкционировать использование СМИБ для управления стратегическими рисками, связанными с потерей интеллектуальной собственности, ущербом репутации и финансовыми потерями, связанными с нарушением конфиденциальности, целостности или доступности информации.

СМИБ может обеспечить руководящий орган управленческой информацией о рисках для организационной структуры и об эффективности СМИБ.

Руководящий орган должен:

- утверждать создание каждой СМИБ;

- определять область применения каждой СМИБ и область сертификации (эти области могут отличаться);

- обеспечивать координацию каждой СМИБ, определяя цели, требования, роли и ресурсы;

- принимать решения о приемлемых уровнях остаточного риска или соответствующих методах обработки риска;

- предоставить каждой СМИБ каналы связи и полномочия использовать эти каналы для передачи соответствующей информации всем заинтересованным сторонам и лицам в пределах действия СМИБ.

8.2 Варианты (см. приложение В)

Тип А: Организация составляет единое целое с организационной структурой

Если единственная действующая система менеджмента соответствует ISO/IEC 27001, ее можно использовать для предоставления информации о рисках и, таким образом, позволять организации управлять информационными рисками. Однако для поддержки управления ИТ, управления финансами, операционного управления и других видов управления по-прежнему будут использоваться другие процессы.

В случае, когда СМИБ применяется ко всей организационной структуре:

- процессы руководства деятельностью, описанные в разделе 7.3, неизменны;

- высшее руководство помимо руководства деятельностью по обеспечению ИБ несет ответственность за руководство другой деятельностью, например за корпоративное управление.

Согласование целей ИБ организации с общими целями организационной структуры, вероятно, будет простым, поскольку высшее руководство отвечает и за те, и за другие. Если роль ответственного за руководство деятельностью по обеспечению ИБ совмещается с ролью ответственного за менеджмент ИБ, то необходимо обеспечить, чтобы отчетности за установление политики и за ее выполнение были должным образом отделены друг от друга.

Тип В: Организация охватывает часть большой организационной структуры

В некоторых случаях организации входят в состав большой организационной структуры. Поскольку деятельность по управлению обычно распространяется на юридическое лицо в целом, корпорацию, благотворительную организационную структуру, государственную организационную структуру или другую организационную структуру, руководство деятельностью такой организационной структуры расширяется в этом случае за пределы применения СМИБ. Организационная структура может иметь несколько СМИБ в своих границах. Таким образом, руководящий орган может управлять несколькими СМИБ. Большая часть настоящего стандарта написана с учетом такого подхода.

Четыре процесса управления, описанные в 7.3, остаются актуальными.

Однако в зависимости от отношений между организацией (организациями) и родительской организационной структурой может иметь место одна из следующих ситуаций:

- каждая организация действует в качестве автономной части родительской организационной структуры и поэтому имеет свои собственные бизнес-цели. В этом случае цели ИБ организации должны быть согласованы с ее собственными бизнес-целями;

- каждая организация ответственна за достижение одной или нескольких бизнес-целей ее родительской организационной структуры. В этом случае цели ИБ организации должны быть согласованы с бизнес-целями ее родительской организационной структуры;

- на каждую организацию возложена ответственность за вопрос управления рисками ИБ от имени родительской организационной структуры. В этом случае цели ИБ организации должны быть определены родительской организационной структурой, что обеспечивает согласованность с бизнес-целями родительской организационной структуры.

Кроме того, необходимо также учитывать взаимоотношения между высшим руководством каждой организации и руководящим органом родительской организационной структуры. Состав высшего руководства и состав руководящего органа может быть одним и тем же, в них могут входить одни и те же лица или же они могут не иметь ничего общего. Для определения, кого следует назначать на роли членов руководящего органа и заинтересованных сторон, можно использовать рисунок В.1.

Тип С: Организация охватывает части нескольких организационных структур

В этой ситуации организация, как обычно, управляется и контролируется высшим руководством, но охватывает несколько организационных структур. Такое возможно в случае, когда более крупная организационная структура управляет группой организаций, которые разделяют общий контекст информационной безопасности и требования для некоторой части своей деятельности, например сбора,

обработки, хранения и использования личных данных для предоставления услуг. Несколько органов управления также могут использовать одну и ту же СМИБ; например, организационная структура может предоставить клиентам в качестве услуги использование СМИБ.

В случае, если организация охватывает части нескольких организационных структур:

- процессы руководства деятельностью, как описано в 7.3, неизменны;
- цели ИБ организации должны быть согласованы с общими бизнес-целями, которые объединяют организационные структуры.

Приложение А
(справочное)

Взаимосвязь руководства деятельностью

Взаимосвязь между руководством деятельностью по обеспечению ИБ и руководством деятельностью по ИТ показана на рисунке А.1.

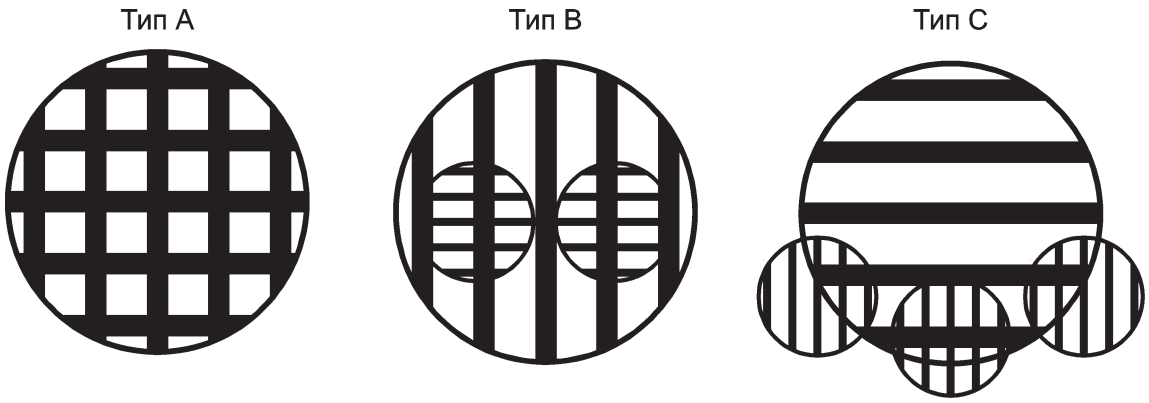
Рисунок А.1 — Связь руководства деятельностью по обеспечению ИБ с руководством деятельностью по ИТ

В то время как руководство деятельностью по ИТ нацелено на ресурсы, необходимые для получения, обработки, хранения и распространения информации, деятельность по обеспечению ИБ обеспечивает конфиденциальность, целостность и доступность информации. Обе схемы руководства деятельностью могут обеспечиваться процессами управления, такими как: оценка, координация, мониторинг и обмен информацией.

Приложение В
(справочное)

Типы организаций систем менеджмента информационной безопасности

Существует три типа отношений между организацией, которая управляет СМИБ, и организационной структурой, которая применяет СМИБ. Кроме прочего, эти отношения влияют как на состав высшего руководства СМИБ, так и на состав руководящего органа организационной структуры. На рисунке В.1 показаны типы отношений, а далее приведены пояснения для каждого типа.



Обозначения

Области действия руководящего органа и высшего руководства СМИБ совпадают

Область действия организационной структуры, включая руководящий орган

Область действия СМИБ, включая высшее руководство

Рисунок В.1 — Возможные отношения организационных структур и их СМИБ

- Тип А: границы организационной структуры и организации совпадают.
Руководящий орган и высшее руководство СМИБ совпадают (совмещены).
- Тип В: организационная структура содержит одну или более организаций.
В руководящий орган может входить несколько членов из каждой СМИБ, но их количество может различаться.
- Тип С: одна СМИБ совместно используется несколькими организационными структурами.

Если организационные структуры имеют прямую заинтересованность в СМИБ, руководящий орган каждой организационной структуры может быть членом высшего руководства СМИБ.

Если СМИБ предоставляется в качестве услуги третьей стороной, в состав высшего руководства СМИБ вряд ли будут входить члены руководящих органов организаций, совместно использующих СМИБ.

Приложение С
(справочное)

Примеры обмена информацией

Один из примеров обмена информацией можно увидеть на фондовых рынках, где компании обязаны раскрывать риски ИБ в соответствии с законами или отраслевыми правилами. Другим примером является отчет по экологическим, социальным и управленческим вопросам (ESG) как средство, с помощью которого организационные структуры могут объяснить заинтересованным сторонам свои усилия с экологической, социальной и экономической точек зрения. В некоторых отчетах ESG описывается подход к защите конфиденциальности данных, деятельности по обеспечению ИБ и управлению кризисами для предотвращения инцидентов ИБ.

При проектировании процесса обмена информацией следует учитывать также непреднамеренные последствия неправильного понимания аудиторией или неверных выводов о дополнительном содержании, а также и то, что сообщения могут дойти до лиц, отличающихся от предполагаемой аудитории.

Большинство компьютеров имеют, как правило, одну или несколько служебных программ, способных обойти меры обеспечения ИБ эксплуатируемых систем и прикладных программ.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов межгосударственным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего межгосударственного стандарта
ISO/IEC 27000	—	*
ISO/IEC 27001	—	*
* Соответствующий межгосударственный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта.		

Библиография

[1] ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements

[2] ISO/IEC 27002:2013, Information security, cybersecurity and privacy protection — Code of practice for information security controls

[3] ISO/IEC 27011:2016, Information security, cybersecurity and privacy protection — Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations

[4] ISO 37001:2016, *Anti-bribery management systems — Requirements with guidance for use*

[5] ISO/IEC 38500:2015, *Information technology — Governance of IT for the organization*

[6] Ohki E., Harada Y., Kawaguchi S., Shiozaki T., Kgaua T., Information Security Governance framework, Proceedings of the first ACM workshop on Information security governance, pp. 1—6, 2009

[7] IT Governance Institute (ITGI), Information Security Governance: Guidance for Information Security Managers: 2008

[8] ITGI, Information Security Governance Guidance for Boards of Directors and Executive Management 2nd Edition: 2006

[9] ITGI, COBIT Control Practices: Guidance to Achieve Control Objective for Successful IT Governance, 2nd Edition: 2007

[10] ISF, Standard of Good Practice for Information Security: 2018

УДК 006.34:004.056:004.056.5:004.056.53 МКС 35.030

Ключевые слова: информационная безопасность, менеджмент информационной безопасности, система менеджмента информационной безопасности (СМИБ), руководство деятельностью по обеспечению информационной безопасности, модель ОКМ (оценка, координация, мониторинг)

Редактор *В.Н. Шмельков*
Технический редактор *И.Е. Черепкова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *М.В. Лебедевой*

Сдано в набор 09.07.2021. Подписано в печать 14.07.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,79. Уч.-изд. л. 2,40.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru