Международный союз электросвязи

МСЭ-Т X.1054

(04/2021)

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

СЕРИЯ X: СЕТИ ПЕРЕДАЧИ ДАННЫХ,
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ
И БЕЗОПАСНОСТЬ

Безопасность информации и сетей –
Управление безопасностью

Информационная безопасность, кибербезопасность и защита конфиденциальности – Общий процесс управления информационной безопасностью

Рекомендация МСЭ-Т X.1054

РЕКОМЕНДАЦИИ МСЭ-Т СЕРИИ X

СЕТИ ПЕРЕДАЧИ ДАННЫХ, ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ И БЕЗОПАСНОСТЬ

СЕТИ ПЕРЕДАЧИ ДАННЫХ ОБЩЕГО ПОЛЬЗОВАНИЯ	X.1–X.199
ВЗАИМОСВЯЗЬ ОТКРЫТЫХ СИСТЕМ	X.200–X.299
ВЗАИМОДЕЙСТВИЕ МЕЖДУ СЕТЯМИ	X.300–X.399
СИСТЕМЫ ОБРАБОТКИ СООБЩЕНИЙ	X.400–X.499
СПРАВОЧНИК	X.500–X.599
ОРГАНИЗАЦИЯ СЕТИ ВОС И СИСТЕМНЫЕ АСПЕКТЫ	X.600–X.699
УПРАВЛЕНИЕ В ВОС	X.700–X.799
БЕЗОПАСНОСТЬ	X.800–X.849
ПРИЛОЖЕНИЯ ВОС	X.850–X.899
ОТКРЫТАЯ РАСПРЕДЕЛЕННАЯ ОБРАБОТКА	X.900–X.999
БЕЗОПАСНОСТЬ ИНФОРМАЦИИ И СЕТЕЙ	
Общие аспекты безопасности	X.1000–X.1029
Безопасность сетей	X.1030–X.1049
Управление безопасностью	**X.1050–X.1069**
Телебиометрия	X.1080–X.1099
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (1)	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды (1)	X.1140–X.1149
Безопасность приложений (1)	X.1150–X.1159
Безопасность одноранговых сетей	X.1160–X.1169
Безопасность сетевой идентификации	X.1170–X.1179
Безопасность IPTV	X.1180–X.1199
БЕЗОПАСНОСТЬ КИБЕРПРОСТРАНСТВА	
Кибербезопасность	X.1200–X.1229
Противодействие спаму	X.1230–X.1249
Управление определением идентичности	X.1250–X.1279
БЕЗОПАСНЫЕ ПРИЛОЖЕНИЯ И УСЛУГИ (2)	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1319
Безопасность умных электросетей	X.1330–X.1339
Сертифицированная электронная почта	X.1340–X.1349
Безопасность интернета вещей (IoT)	X.1350–X.1369
Безопасность интеллектуальных транспортных систем (ИТС)	X.1370–X.1399
Безопасность технологии распределенного реестра (DLT)	X.1400–X.1429
Безопасность приложений (2)	X.1450–X.1459
Безопасность веб-среды (2)	X.1470–X.1489
ОБМЕН ИНФОРМАЦИЕЙ, КАСАЮЩЕЙСЯ КИБЕРБЕЗОПАСНОСТИ	
Обзор кибербезопасности	X.1500–X.1519
Обмен информацией об уязвимости/состоянии	X.1520–X.1539
Обмен информацией о событии/инциденте/эвристических правилах	X.1540–X.1549
Обмен информацией о политике	X.1550–X.1559
Эвристические правила и запрос информации	X.1560–X.1569
Идентификация и обнаружение	X.1570–X.1579
Гарантированный обмен	X.1580–X.1589
Киберзащита	X.1590–X.1599
БЕЗОПАСНОСТЬ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ	
Обзор безопасности облачных вычислений	X.1600–X.1601
Проектирование безопасности облачных вычислений	X.1602–X.1639
Передовой опыт и руководящие указания в области облачных вычислений	X.1640–X.1659
Обеспечение безопасности облачных вычислений	X.1660–X.1679
Другие вопросы безопасности облачных вычислений	X.1680–X.1699
КВАНТОВАЯ СВЯЗЬ	
Терминология	X.1700–X.1701
Квантовый генератор случайных чисел	X.1702–X.1709
Структура безопасности QKDN	X.1710–X.1711
Проектирование безопасности QKDN	X.1712–X.1719
Методы обеспечения безопасности QKDN	X.1720–X.1729
БЕЗОПАСНОСТЬ ДАННЫХ	
Безопасность больших данных	X.1750–X.1759
Защита данных	X.1770–X.1789
БЕЗОПАСНОСТЬ СЕТЕЙ IMT-2020	X.1800–X.1819

Для получения более подробной информации просьба обращаться к перечню Рекомендаций МСЭ-Т.

МЕЖДУНАРОДНЫЙ СТАНДАРТ ИСО/МЭК 27014
РЕКОМЕНДАЦИЯ МСЭ-Т X.1054

Информационная безопасность, кибербезопасность и защита конфиденциальности – Общий процесс управления информационной безопасностью

Резюме

В Рекомендации МСЭ-Т X.1054 | Международном стандарте ИСО/МЭК 27014 приводится руководство по общему процессу управления информационной безопасностью.

Обеспечение информационной безопасности является одной из важных задач организаций, которая усложняется вследствие быстрого развития способов и технологий атак, а также соответствующего усиления регулярного давления.

Неэффективность мер контроля за информационной безопасностью может иметь множество неблагоприятных последствий для организации и соответствующих заинтересованных сторон, включая, помимо прочего, подрыв доверия.

Общее управление информационной безопасностью заключается в использовании ресурсов для эффективного обеспечения информационной безопасности. Оно гарантирует:

- соблюдение директив, относящихся к информационной безопасности; и
- получение руководящим органом достоверной и своевременной отчетности о деятельности, связанной с информационной безопасностью.

Это помогает руководящему органу принимать решения в отношении стратегических задач организации благодаря полученным сведениям по информационной безопасности, которые могут повлиять на выполнение этих задач. Это также гарантирует соответствие стратегии информационной безопасности общим целям объекта.

Руководители и другие работники организаций должны понимать:

- требования к общему процессу управления, влияющие на их работу; и
- способы соблюдения требований к общему процессу управления, когда необходимо действовать.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия	Уникальный идентификатор*
1.0	МСЭ-Т X.1054	07.09.2012 г.	17-я	11.1002/1000/11594
2.0	МСЭ-Т X.1054	30.04.2021 г.	17-я	11.1002/1000/14248

Ключевые слова

Информационная безопасность, общий процесс управления информационной безопасностью, управление информационной безопасностью, ISMS.

* Для получения доступа к Рекомендации наберите в адресном поле вашего браузера URL http://handle.itu.int/, после которого укажите уникальный идентификатор Рекомендации. Например, http://handle.itu.int/11.1002/1000/11830-en.

ПРЕДИСЛОВИЕ

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи и информационно-коммуникационных технологий (ИКТ). Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним в целях стандартизации электросвязи на всемирной основе.

На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам.

Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ.

В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ПРИМЕЧАНИЕ

В настоящей Рекомендации термин "администрация" используется для краткости и обозначает как администрацию электросвязи, так и признанную эксплуатационную организацию.

Соблюдение положений данной Рекомендации осуществляется на добровольной основе. Однако данная Рекомендация может содержать некоторые обязательные положения (например, для обеспечения функциональной совместимости или возможности применения), и в таком случае соблюдение Рекомендации достигается при выполнении всех указанных положений. Для выражения требований используются слова "следует", "должен" (shall) или некоторые другие обязывающие выражения, такие как "обязан" (must), а также их отрицательные формы. Употребление таких слов не означает, что от какой-либо стороны требуется соблюдение положений данной Рекомендации.

ПРАВА ИНТЕЛЛЕКТУАЛЬНОЙ СОБСТВЕННОСТИ

МСЭ обращает внимание на вероятность того, что практическое применение или выполнение настоящей Рекомендации может включать использование заявленного права интеллектуальной собственности. МСЭ не занимает какую бы то ни было позицию относительно подтверждения, действительности или применимости заявленных прав интеллектуальной собственности независимо от того, доказываются ли такие права членами МСЭ или другими сторонами, не относящимися к процессу разработки Рекомендации.

На момент утверждения настоящей Рекомендации МСЭ не получил извещения об интеллектуальной собственности, защищенной патентами, которые могут потребоваться для выполнения настоящей Рекомендации. Однако те, кто будет применять Рекомендацию, должны иметь в виду, что вышесказанное может не отражать самую последнюю информацию, и поэтому им настоятельно рекомендуется обращаться к патентной базе данных БСЭ по адресу http://www.itu.int/ITU-T/ipr/.

СОДЕРЖАНИЕ

Введение

Международный союз электросвязи (МСЭ) является специализированным учреждением Организации Объединенных Наций в области электросвязи. Сектор стандартизации электросвязи МСЭ (МСЭ-Т) – постоянный орган МСЭ. МСЭ-Т отвечает за изучение технических, эксплуатационных и тарифных вопросов и за выпуск Рекомендаций по ним в целях стандартизации электросвязи на всемирной основе. На Всемирной ассамблее по стандартизации электросвязи (ВАСЭ), которая проводится каждые четыре года, определяются темы для изучения исследовательскими комиссиями МСЭ-Т, которые, в свою очередь, вырабатывают Рекомендации по этим темам. Утверждение Рекомендаций МСЭ-Т осуществляется в соответствии с процедурой, изложенной в Резолюции 1 ВАСЭ. В некоторых областях информационных технологий, которые входят в компетенцию МСЭ-Т, необходимые стандарты разрабатываются на основе сотрудничества с ИСО и МЭК.

ИСО (Международная организация по стандартизации) и МЭК (Международная электротехническая комиссия) образуют специализированную систему международной стандартизации. Национальные органы, которые являются членами ИСО или МЭК, участвуют в разработке Рекомендаций | Международных стандартов в различных сферах технической деятельности через посредство технических комитетов, учрежденных соответствующей организацией. Технические комитеты ИСО и МЭК сотрудничают в областях, представляющих обоюдный интерес. Участие в этой совместной работе принимают и другие правительственные и неправительственные международные организации. В сфере информационной безопасности, кибербезопасности и защиты конфиденциальности ИСО и МЭК учредили Объединенный технический комитет – ОТК 1 ИСО/МЭК.

Проект настоящей Рекомендации | Международного стандарта подготовлен в соответствии с правилами, приведенными в Директивах ИСО/МЭК, часть 2.

Основная задача Объединенного технического комитета заключается в подготовке настоящей Рекомендации | Международного стандарта. Проекты Рекомендаций | Международных стандартов, принимаемые Объединенным техническим комитетом, направляются для голосования в национальные органы. Для публикации в качестве международного стандарта необходимо, чтобы проект получил одобрение не менее 75% национальных органов, участвовавших в голосовании.

Следует иметь в виду, что некоторые части настоящей Рекомендации | Международного стандарта могут быть предметом патентных прав. МСЭ, ИСО или МЭК не несут ответственности за выявление таких патентных прав.

Рекомендация МСЭ-Т X.1054 | стандарт ИСО/МЭК 27014 подготовлена Подкомитетом SC 27 (Информационная безопасность, кибербезопасность и защита конфиденциальности) Объединенного технического комитета ОТК 1 ИСО/МЭК (Информационные технологии) совместно с ИК17 МСЭ-Т.

МЕЖДУНАРОДНЫЙ СТАНДАРТ
РЕКОМЕНДАЦИЯ МСЭ-Т

Информационная безопасность, кибербезопасность и защита конфиденциальности – Общий процесс управления информационной безопасностью

1 Сфера применения

В настоящей Рекомендации | Международном стандарте приводится руководство по концепциям, задачам и процессам общего управления информационной безопасностью, с помощью которых организации могут оценивать, направлять и контролировать свои внутренние процессы, связанные с информационной безопасностью, а также обмениваться соответствующей информацией о них.

Целевая аудитория настоящего документа:

- руководящий орган и высшее руководство;
- лица, ответственные за оценку, руководство и контроль системы управления информационной безопасностью (ISMS) на основе стандарта ИСО/МЭК 27001;
- лица, ответственные за управление информационной безопасностью вне сферы применения ISMS на основе стандарта ИСО/МЭК 27001, но в рамках общего управления.

Настоящая Рекомендация | Международный стандарт применима к организациям всех видов и размеров.

Все ссылки на ISMS в настоящем документе относятся к ISMS на основе стандарта ИСО/МЭК 27001.

Настоящая Рекомендация | Международный стандарт ориентирована на организации ISMS трех типов, указанных в Приложении B. Однако она может использоваться и организациями других типов.

2 Нормативные справочные документы

Нижеследующие Рекомендации и международные стандарты содержат положения, которые путем ссылки на них в данном тексте образуют положения настоящей Рекомендации | Международного стандарта. На момент публикации указанные издания были действительны. Все Рекомендации и стандарты подвергаются пересмотру, поэтому сторонам соглашений, основанных на данной Рекомендации | Международном стандарте, следует рассматривать возможность применения самых последних изданий перечисленных ниже Рекомендаций и стандартов. Члены МЭК и ИСО ведут регистры действующих в настоящее время международных стандартов. Бюро стандартизации электросвязи МСЭ ведет список действующих в настоящее время Рекомендаций МСЭ-Т.

– ISO/IEC 27000: действующая версия, *Information technology – Security techniques – Information security management systems – Overview and vocabulary.*
– ISO/IEC 27001: действующая версия, *Information technology – Security techniques – Information security management systems – Requirements.*

3 Определения

Для целей настоящей Рекомендации | Международного стандарта применяются термины и определения, содержащиеся в стандартах ИСО/МЭК 27000, а также нижеследующие термины и определения.

ИСО, МЭК и МСЭ ведут терминологические базы данных для использования при стандартизации, которые доступны по следующим адресам:

- IEC Electropedia: http://www.electropedia.org/;
- онлайн-платформа ИСО: http://www.iso.org/obp;
- термины и определения МСЭ: http://www.itu.int/go/terminology-database.

3.1 объект (entity): Организация (3.2) и другие органы или стороны.

ПРИМЕЧАНИЕ. – Объектом может быть группа компаний, отдельная компания, некоммерческая компания и др. Объект имеет полномочия по общему управлению организацией. Объект может быть идентичен организации, например, в небольших компаниях.

3.2 организация (organization): Та часть объекта (3.1), которая обеспечивает функционирование и управление ISMS.

3.3 руководящий орган (governing body): Лицо или группа лиц, которые несут ответственность за показатели деятельности объекта и его соответствие установленным требованиям.

ПРИМЕЧАНИЕ. – ИСТОЧНИК: ISO/IEC 27000:2018, пункт 3.24, изменено – слово "организация" заменено на "объект".

3.4 высшее руководство (top management): Лицо или группа лиц, которые руководят и осуществляют контроль за организацией (3.2) на высшем уровне.

ПРИМЕЧАНИЕ 1. – Источник: ISO/IEC 9001.

ПРИМЕЧАНИЕ 2. – Высшее руководство обладает правом делегировать полномочия и предоставлять ресурсы в пределах организации.

ПРИМЕЧАНИЕ 3. – Если сфера применения системы управления охватывает только часть объекта, то высшим руководством считаются те, кто руководит и осуществляет контроль за деятельностью этой части объекта. В данной ситуации высшее руководство подотчетно руководящему органу объекта.

ПРИМЕЧАНИЕ 4. – В зависимости от размера и ресурсов организации в роли высшего руководства может выступать руководящий орган.

ПРИМЕЧАНИЕ 5. – Высшее руководство подотчетно руководящему органу [ИСТОЧНИК: ISO/IEC 27000:2018, пункт 3.75].

ПРИМЕЧАНИЕ 6. – Определения терминов "руководящий орган" и "высшее руководство" также содержатся в стандарте ИСО/МЭК 37001.

4 Сокращения

Для целей настоящей Рекомендации | Международного стандарта приняты следующие сокращения.

ISMS	Information Security Management System		Система управления информационной безопасностью
IT	Information Technology	ИТ	Информационные технологии

5 Назначение и структура настоящей Рекомендации | Международного стандарта

Настоящая Рекомендация | Международный стандарт содержит описание методов общего управления информационной безопасностью в рамках ISMS на основе стандарта ИСО/МЭК 27001 и возможных связей этой деятельности с другой деятельностью по общему управлению, выходящей за рамки ISMS. В ней описываются четыре основных процесса – оценка, руководство, контроль и информирование, по которым ISMS может быть структурирована внутри организации, и предлагаются подходы к интегрированию общего процесса управления информационной безопасностью в деятельность по общему управлению организацией в рамках каждого из этих процессов. И наконец, в Приложении А рассматриваются взаимосвязи между процессами общего управления организацией, общего управления информационными технологиями и общего управления информационной безопасностью.

По определению ISMS охватывает всю организацию (см. ИСО/МЭК 27000). Она может охватывать весь объект или его часть. Это показано на рисунке B.1.

6 Стандарты общего управления и стандарты управления

6.1 Обзор

Общее управление информационной безопасностью – это механизм, посредством которого руководящий орган обеспечивает общее руководство и контроль за деятельностью, оказывающей влияние на безопасность информации организации. В рамках такого руководства и контроля основной упор делается на условиях, при которых неадекватная защита информации может подорвать способность организации добиваться выполнения стоящих перед ней общих задач. Как правило, руководящий орган выполняет свои задачи общего управления:

- осуществляя руководство путем установления стратегий и политики;
- контролируя показатели деятельности организации; а также
- оценивая предложения и планы, разработанные менеджерами.

Управление информационной безопасностью ассоциируется с обеспечением достижения целей организации, указанных в установленных руководящим органом стратегиях и политике. Сюда можно отнести и взаимодействие с руководящим органом:

- путем представления предложений и планов на рассмотрение руководящего органа; и

- путем предоставления руководящему органу информации, касающейся показателей деятельности организации.

Для обеспечения эффективности общего управления информационной безопасностью необходимо, чтобы как члены руководящего органа, так и менеджеры согласованно выполняли свои функции.

6.2 Деятельность по общему управлению в рамках ISMS

Стандарт ИСО/МЭК 27001 определяет требования по созданию, внедрению, поддержке и постоянному совершенствованию системы управления информационной безопасностью в контексте организации. Он также содержит требования по оценке и обработке рисков информационной безопасности, адаптированные к потребностям организации.

В стандарте ИСО/МЭК 27001 термин "общее управление" (governance) не используется, но определен ряд требований, относящихся к деятельности по общему управлению. Ниже перечислены примеры такой деятельности. Термины "организация" и "высшее руководство", как уже отмечалось, относятся к сфере применения ISMS на основе стандарта ИСО/МЭК 27001.

- Пункт 4.1 ИСО/МЭК 27001:2013 требует, чтобы организация определила, чего она стремится достичь, то есть свои цели и задачи в области информационной безопасности. Они должны быть связаны с общими целями и задачами объекта и способствовать их достижению/решению. Это относится к задачам общего управления 1, 3 и 4, изложенным в пункте 7.2 настоящей Рекомендации | Международного стандарта.
- Пункт 4.2 ИСО/МЭК 27001:2013 требует, чтобы организация определила заинтересованные стороны, имеющие отношение к ее ISMS, и потребности этих заинтересованных сторон, относящиеся к информационной безопасности. Это относится к задаче общего управления 4, изложенной в пункте 7.2 настоящей Рекомендации | Международного стандарта.
- Пункт 4.3 ИСО/МЭК 27001:2013 требует, чтобы организация определила границы и применимость ISMS для установления сферы ее применения с учетом внешних и внутренних документов, требований, взаимодействия и зависимостей. В нем также говорится, что организация должна встроить в свою систему управления информационной безопасностью требования и ожидания заинтересованных сторон, а также внешние и внутренние документы (например, законы, нормативные положения и контракты). Это относится к задаче общего управления 1, изложенной в пункте 7.2 настоящей Рекомендации | Международного стандарта.
- В пункте 5 ИСО/МЭК 27001:2013 говорится, что организация должна установить политику и цели и интегрировать информационную безопасность в свои процессы (к которым можно отнести и процессы общего управления). Он требует от организации предоставления надлежащих ресурсов для управления информационной безопасностью и информирования о важности такого управления. Что особенно важно, в этом разделе также отмечается, что организация должна направлять и поддерживать деятельность людей, способствующих повышению эффективности ISMS, а также поддерживать других руководителей в реализации их функций в сфере их ответственности. В пункте 5 ИСО/МЭК 27001:2013 содержатся инструкции по установлению политики и назначению ответственных за управление информационной безопасностью и предоставлению соответствующей отчетности. Это относится к задачам общего управления 1 и 3, изложенным в пункте 7.2 настоящей Рекомендации | Международного стандарта.
- В пункте 6 ИСО/МЭК 27001:2013 рассматривается подход к управлению рисками организации и говорится, что организация должна определить те риски и возможности, которые необходимо учитывать для обеспечения эффективности ISMS. В нем вводится понятие ответственных за риски и рассматриваются их обязанности в контексте деятельности организации по управлению рисками и утверждению мер по обработке рисков. Этот раздел также требует от организации постановки задач информационной безопасности. Это относится к задаче общего управления 2, изложенной в пункте 7.2 настоящей Рекомендации | Международного стандарта.
- В пункте 7 ИСО/МЭК 27001:2013 указывается, что работники должны компетентно выполнять свои обязанности в области информационной безопасности, и содержится требование к процессам информирования в рамках организации. Это относится к задаче общего управления 5, изложенной в пункте 7.2 настоящей Рекомендации | Международного стандарта.
- В пункте 8 ИСО/МЭК 27001:2013 определяется ответственность организации за планирование, внедрение и контроль за ее ISMS, включая соглашения со сторонними поставщиками. Это относится к задачам общего управления 4 и 6, изложенным в пункте 7.2 настоящей Рекомендации | Международного стандарта.

- В пункте 9 ИСО/МЭК 27001:2013 содержатся требования к контролю и отчетности по всем соответствующим аспектам ISMS, внутренним проверкам, а также к анализу высшим руководством и руководящим органом эффективности функционирования ISMS и принимаемым ими решениям по этому вопросу, включая любые необходимые изменения. Это относится к задаче общего управления 6, изложенной в пункте 7.2 настоящей Рекомендации | Международного стандарта.
- В пункте 10 ИСО/МЭК 27001:2013 говорится о выявлении и устранении несоответствий, требованиях по выявлению возможностей для постоянного совершенствования и мерах по использованию этих возможностей. Это относится к задаче общего управления 4, изложенной в пункте 7.2 настоящей Рекомендации | Международного стандарта.

6.3 Другие соответствующие стандарты

Стандарт ИСО/МЭК 38500 содержит руководящие принципы для членов руководящих органов организаций по эффективному, действенному и приемлемому использованию информационных технологий в своих организациях. Он также содержит руководство для тех, кто консультирует или информирует руководящие органы по вопросам общего управления ИТ или помогает им в общем управлении ИТ.

6.4 Цепочка управления внутри организации

Эти цепочки в точности соответствуют процессам общего управления организацией, описанным в разделе 7. Последние два элемента в списке эквивалентны соответствующим аспектам общего управления в контексте информационной безопасности:

- согласование задач информационной безопасности с бизнес-задачами;
- управление рисками информационной безопасности в соответствии с этими задачами информационной безопасности;
- недопущение конфликтов интересов в управлении информационной безопасностью;
- предотвращение использования информационных технологий организации для причинения ущерба другим организациям.

7 Общее управление объектом и общее управление информационной безопасностью

7.1 Обзор

Общее управление в пределах объекта осуществляется по многим направлениям, включая информационную безопасность, информационные технологии, технику безопасности, качество и финансы. Каждое такое направление – составная часть общих задач управления объектом, а следовательно, все они должны соответствовать дисциплине объекта. Иногда сферы применения моделей общего управления пересекаются. В пунктах 7.2 и 7.3 описываются задачи и процессы, связанные с общим процессом управления информационной безопасностью, которые применимы к общему управлению в любой области.

Система ISMS предназначена для управления рисками, связанными с информацией. Она не имеет непосредственного отношения к таким вопросам, как рентабельность, закупки, использование и реализация активов или результативность других процессов, хотя и должна соответствовать любым задачам организации, относящимся к этим вопросам.

7.2 Задачи управления

7.2.1 Задача 1. Внедрение всесторонней комплексной информационной безопасности на уровне всего объекта

Общий процесс управления информационной безопасностью должен обеспечивать, чтобы решаемые задачи информационной безопасности были всесторонними и комплексными. Информационной безопасностью следует заниматься на уровне объекта, а при принятии решений следует учитывать приоритеты объекта. Деятельность, касающуюся физической и логической безопасности, следует тесно координировать. Однако при этом не требуется единый набор мер безопасности или единая система управления информационной безопасностью (ISMS) для всего объекта.

Для обеспечения информационной безопасности на уровне всего объекта необходимо ввести ответственность и подотчетность за информационную безопасность по всем направлениям деятельности объекта. Это может выходить за рамки общепринятых границ деятельности объекта, например охватывая информацию, хранящуюся или передаваемую внешними сторонами.

7.2.2 Задача 2. Принятие решений с использованием подхода, основанного на оценке рисков

Общий процесс управления информационной безопасностью должен основываться на выполнении обязательств по соблюдению требований, а также на решениях, основанных на конкретных рисках, характерных для объекта. Определение приемлемой степени безопасности должно основываться на склонности объекта к риску, включая риск утраты конкурентных преимуществ, риски в области соответствия и ответственности, перебои в работе, ущерб репутации и финансовые потери.

Управление рисками информационной безопасности должно быть согласовано в рамках всего объекта с учетом возможных неблагоприятных финансовых, эксплуатационных и репутационных последствий нарушений и несоответствия. Кроме того, управление рисками информационной безопасности следует включить в общий подход объекта к управлению рисками, чтобы оно не осуществлялось изолированно и не создавало путаницу, например отобразить в методологии объекта или добавить стратегические информационные риски в реестр рисков объекта.

В рамках общего процесса управления безопасностью следует выделять соответствующие ресурсы для внедрения управления информационными рисками.

7.2.3 Задача 3. Организация руководства закупками

При осуществлении новых видов деятельности, включая, помимо прочего, любые инвестиции, закупки, слияние, внедрение новых технологий, соглашения об аутсорсинге и контракты с внешними поставщиками, следует надлежащим образом оценивать влияние риска в области информационной безопасности.

Чтобы оптимизировать закупки, связанные с информационной безопасностью, для поддержки задач объекта, руководящему органу следует обеспечить интегрирование вопроса информационной безопасности в существующие процессы объекта, включая управление проектами, снабжение, финансовые затраты, соответствие нормативно-правовым требованиям и стратегическое управление рисками.

Высшему руководству ISMS необходимо разработать стратегию информационной безопасности, основанную на задачах организации, обеспечивая согласование требований объекта с требованиями к информационной безопасности организации и тем самым удовлетворение текущих и будущих потребностей заинтересованных сторон.

7.2.4 Задача 4. Обеспечение соответствия внутренним и внешним требованиям

Общий процесс управления информационной безопасностью должен обеспечивать, чтобы политика и практика в сфере информационной безопасности соответствовали требованиям заинтересованных сторон. Они могут включать законы и нормативные акты, а также договорные требования и внутренние обязательства.

Для решения вопросов, связанных с соответствием и соблюдением положений, высшее руководство может получить заверения в том, что деятельность в сфере информационной безопасности удовлетворительным образом соответствует внутренним и внешним требованиям, поручив проведение независимого аудита в области безопасности.

7.2.5 Задача 5. Содействие формированию культуры безопасности

Общий процесс управления информационной безопасностью должен быть основан на [корпоративной] культуре объекта, в том числе на появляющихся потребностях всех заинтересованных сторон, поскольку поведение людей является одной из основных составляющих обеспечения надлежащего уровня информационной безопасности. При отсутствии необходимой координации задачи, функции, сферы ответственности и ресурсы могут вступить в противоречие друг с другом, что приведет к невозможности достижения каких бы то ни было целей. Следовательно, очень важны согласование и совместные действия различных заинтересованных сторон.

Для создания культуры позитивного отношения к информационной безопасности высшему руководству следует требовать проведения координации и содействовать координации деятельности заинтересованных сторон, а также поддерживать такую координацию в целях согласованного руководства информационной безопасностью. Это обеспечивает разработку программ по обучению, профессиональной подготовке и повышению информированности в сфере безопасности. Ответственность за информационную безопасность должна быть включена в функции персонала и других сторон, и они должны обеспечивать успешное функционирование каждой ISMS, приняв на себя эту ответственность.

7.2.6 Задача 6. Обеспечение соответствия показателей безопасности текущим и будущим требованиям объекта

Общий процесс управления информационной безопасностью должен обеспечить соответствие подхода, принятого для защиты информации, целям обеспечения работы объекта, предоставив согласованные уровни информационной безопасности. Показатели безопасности следует контролировать и поддерживать на уровнях, которые необходимы для выполнения нынешних и будущих требований.

Для рассмотрения результативности информационной безопасности с точки зрения общего процесса управления руководящему органу следует оценить такую результативность в отношении ее воздействия на уровне объекта, а не только эффективность и действенность контроля безопасности.

В каждой ISMS высшее руководство ISMS должно требовать выполнения программы измерения показателей для контроля, аудита и определения возможностей их улучшения. Руководящему органу следует связать показатели информационной безопасности с показателями деятельности организации и объекта.

7.3 Процессы

7.3.1 Общие положения

Руководящий орган в рамках объекта осуществляет процессы оценки, руководства, контроля и информирования. На рисунке 1 показана взаимосвязь между этими процессами.

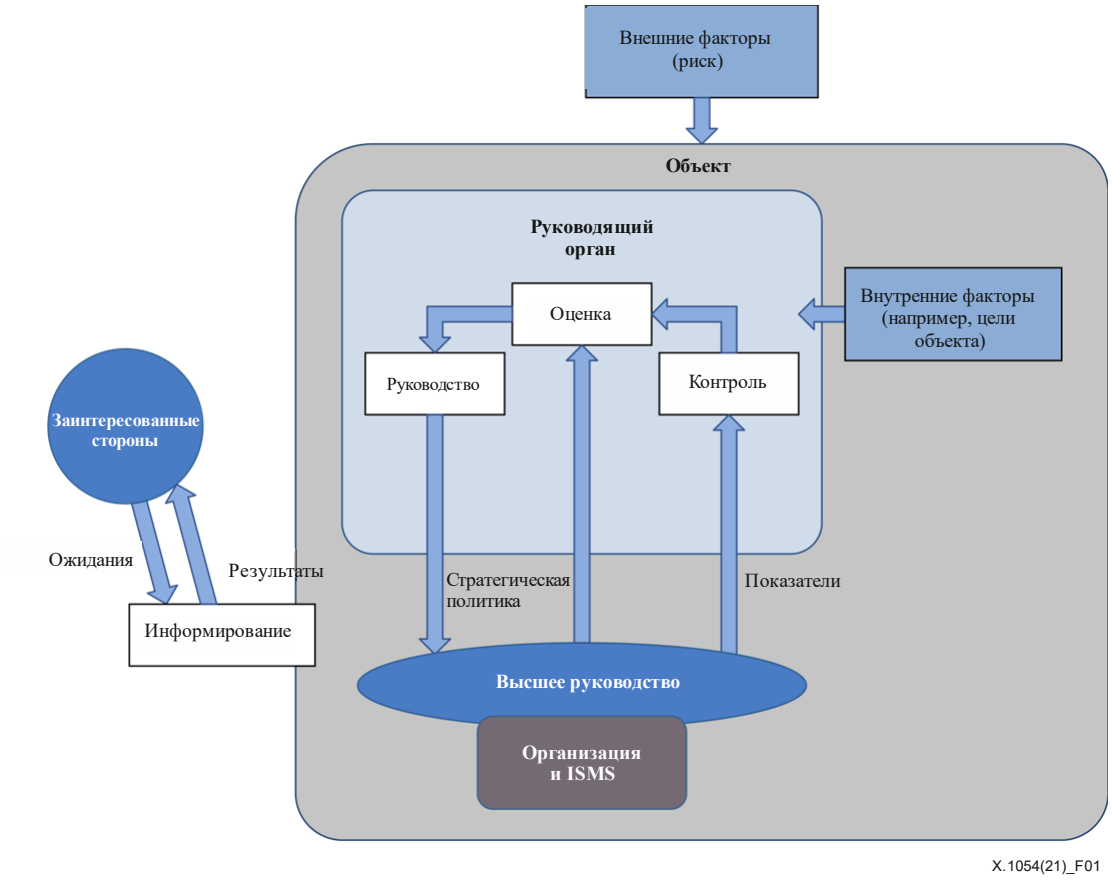

Рисунок 1 – Модель общего управления для объекта с одной ISMS

ПРИМЕЧАНИЕ 1. – Определение "организация" [3.2] означает, что высшее руководство всегда полностью вовлечено в деятельность организации.

ПРИМЕЧАНИЕ 2. – Объект может содержать более одной ISMS, и некоторые управляемые части объекта могут не входить в состав ISMS. См. раздел 8 и Приложение B.

7.3.2 Оценка

Оценка – это общий процесс управления, при котором рассматривается нынешнее и прогнозируемое достижения целей на основе текущих процессов и запланированных изменений, а также определяется, требуются ли какие-нибудь корректировки для оптимизации достижения стратегических целей в будущем.

Для осуществления процесса оценки:

- руководящему органу объекта следует:
  - обеспечить, чтобы в инициативах учитывались соответствующие риски и возможности;
  - реагировать на данные измерений и отчеты по информационной безопасности и ISMS, давая определения и устанавливая приоритеты решения требуемых задач в контексте каждой ISMS (с учетом требований, предъявляемых внешним окружением ISMS); и
- высшему руководству каждой ISMS следует:
  - обеспечить, чтобы информационная безопасность адекватным образом поддерживала и подкрепляла задачи объекта;
  - представлять на утверждение руководящему органу новые проекты в области информационной безопасности, которые окажут существенное воздействие.

7.3.3 Руководство

Руководство – это общий процесс управления, с помощью которого руководящий орган дает распоряжения по поводу задач и стратегии объекта. Руководство может включать изменения в уровнях снабжения ресурсами, распределении ресурсов, установлении приоритетов деятельности, а также в утверждении политики, принятии материальных рисков и планов управления рисками.

Для осуществления процесса руководства:

- руководящему органу следует:
  - установить общее стратегическое направление и цели деятельности объекта;
  - определить склонность объекта к риску;
  - утвердить стратегию информационной безопасности; и
- высшему руководству каждой ISMS следует:
  - выделить необходимые инвестиции и ресурсы;
  - согласовать задачи организации в области информационной безопасности с задачами объекта;
  - распределить роли и обязанности в области информационной безопасности;
  - разработать политику в области информационной безопасности.

ПРИМЕЧАНИЕ. – Готовность к принятию рисков – уровень и тип риска, который организация готова принять или сохранить. [8]

7.3.4 Контроль

Контроль – это общий процесс управления, который дает руководящему органу возможность оценивать достижение стратегических целей.

Для осуществления процесса контроля:

- руководящему органу следует:
  - получить отчет по эффективности функционирования каждой ISMS;
  - оценивать их в контексте приоритетов объекта;
  - информировать высшее руководство каждой ISMS о приоритетах; и
- высшему руководству каждой ISMS следует:
  - оценивать эффективность деятельности по управлению информационной безопасностью;
  - обеспечивать соответствие внутренним и внешним требованиям;
  - рассматривать вопросы, связанные с изменением объекта, правовой и регуляторной средой и любым потенциальным воздействием на информационные риски;
  - выбрать подходящие показатели эффективности и требовать своевременного представления отчетности по организации;
  - обеспечить, чтобы руководящему органу сообщалось о результатах деятельности в области информационной безопасности;
  - предупреждать руководящий орган о новых событиях, сказывающихся на информационных рисках и информационной безопасности

Для рассмотрения результативности информационной безопасности с точки зрения общего процесса управления высшему руководству следует оценить такую результативность в отношении ее воздействия на уровне организации и объекта, а не только эффективность и действенность контроля безопасности. Это можно сделать путем внедрения программы измерения показателей для контроля, аудита и определения возможностей их улучшения, увязывая деятельность в сфере информационной безопасности с результатами деятельности организации и объекта.

7.3.5 Информирование

Информирование – это двунаправленный общий процесс управления, с помощью которого руководящий орган и заинтересованные стороны обмениваются информацией, соответствующей их конкретным потребностям.

Одним из методов, который можно использовать для информирования, является сообщение о статусе информационной безопасности с указанием деятельности и вопросов в области информационной безопасности для заинтересованных сторон.

Одна из целей информирования – дать объектам возможность отчитываться перед заинтересованными сторонами, такими как акционеры. Это приобретает все большую важность, и сегодня организации предоставляют информацию о внедрении и поддержании управления информационной безопасностью, а также о его эффективности при управлении рисками. Точно так же в случае инцидента, связанного с информационной безопасностью, объектам следует объяснить своим заинтересованным сторонам – и отдельно, в зависимости от ситуации, общественности – последствия и причину этого инцидента, а также изменения в мерах и средствах управления, которые необходимо осуществить для исключения риска повторных инцидентов.

Информирование может осуществляться разными методами. Оно также может быть разным по содержанию и быть ориентировано на различные аудитории. Любое информирование должно учитывать соответствующую аудиторию, и сообщение должно быть таким, чтобы оно было понятно целевой аудитории. Затем эти два фактора следует использовать для определения содержания сообщений, а также каналов, используемых для донесения сообщений до целевой аудитории. Один пример приведен в Приложении С.

Для осуществления процесса информирования:

- руководящему органу следует:
  - сообщать внешним заинтересованным сторонам, что объект использует уровень информационной безопасности, соразмерный характеру его деятельности и приоритетам;
  - выявлять и устанавливать приоритетность регуляторных обязательств, ожиданий заинтересованных сторон и требований объекта в отношении информационной безопасности;
  - консультировать высшее руководство каждой ISMS по любым вопросам, требующим его внимания и принятия решений;
  - подробно информировать соответствующие заинтересованные стороны о задачах, которые необходимо решить в поддержку приоритетов информационной безопасности;
  - способствовать развитию позитивной культуры информационной безопасности;
  - обучать и информировать персонал и других лиц, занятых в ISMS, об их обязанностях.

8 Требования руководящего органа к ISMS

8.1 Организация и ISMS

Руководящему органу следует требовать, чтобы конструктивное решение одной или нескольких систем ISMS поддерживало стоящие перед объектом задачи. Задачи каждой ISMS могут совпадать с задачами материнского объекта или отличаться от них в зависимости от размера, масштаба и структуры всего объекта, но они должны быть согласованы. Возможные взаимосвязи между общим процессом управления информационной безопасностью и общим процессом управления информационными технологиями показаны в Приложении А.

Руководящему органу также следует требовать, чтобы конструктивное решение каждой ISMS разрабатывалось в соответствии с общей политикой и процессами объекта, включая управление рисками. Для ISMS может быть целесообразно использовать тот же процесс оценки рисков, что и для руководящего органа, чтобы обеспечить четкую передачу информации о рисках. Если руководящий орган использует процесс оценки рисков, не соответствующий требованиям стандарта ИСО/МЭК 27001, то организация, если она желает достичь соответствия таким требования, должна использовать для своей ISMS отличный от применяемого объектом подход к оценке рисков и согласовать способ передачи информации о рисках руководящему органу в форме, совместимой с подходом руководящего органа. В качестве альтернативы руководящий орган может принять

решение об изменении существующего процесса оценки рисков объекта для приведения его в соответствие с требованиями стандарта ИСО/МЭК 27001.

Руководящий орган может дать указание использовать ISMS для управления стратегическими рисками, связанными с потерей интеллектуальной собственности, ущербом для репутации, а также финансовыми потерями, вызванными причиненным ущербом для конфиденциальности, целостности или доступности информации.

ISMS может предоставлять руководящему органу административную информацию:

- по рискам для объекта;
- по эффективности ISMS.

Руководящий орган должен:

- одобрить создание каждой ISMS;
- определить область применения и область сертификации каждой ISMS (эти области могут различаться);
- обеспечить руководство каждой ISMS, включая определение целей, требований, функций и ресурсов;
- принимать решения о приемлемых уровнях остаточного риска или подходящих методах обработки рисков;
- обеспечить каждую ISMS каналами связи и полномочиями для передачи по этим каналам соответствующей информации заинтересованным сторонам и всем, кто входит в сферу применения этой ISMS.

8.2 Сценарии информирования (см. Приложение B)

8.2.1 Тип A. Организация ISMS – это весь объект

Когда имеется только одна система управления, соответствующая стандарту ИСО/МЭК 27001, она может использоваться для предоставления информации о рисках и таким образом позволить организации осуществлять общее управление информационным риском. Однако процессы, используемые при общем управлении ИТ, общем финансовом управлении, общем оперативном управлении и других видах общего управления, остаются разными.

В том случае, когда организация ISMS распространяется на весь объект:

- процессы общего управления, описанные в пункте 7.3, остаются неизменными;
- высшее руководство в дополнение к общему управлению информационной безопасностью несет ответственность, например, за корпоративное управление.

Согласовать задачи организации в области информационной безопасности с общими задачами объекта скорее всего будет легко, поскольку высшее руководство несет ответственность за то и другое. Если на одно и то же должностное лицо возложена ответственность как за общее управление, так и за управление информационной безопасностью, необходимо дать надлежащие рекомендации, чтобы гарантировать, что ответственность за определение политики и за ее исполнение была должным образом разделена.

8.2.2 Тип B. Организация ISMS является частью более крупного объекта

Некоторые организации ISMS являются частью более крупного объекта. Поскольку деятельность по общему управлению обычно распространяется на все юридическое лицо, корпорацию, благотворительную организацию, государственное учреждение или другой объект, общее управление этим объектом в данном случае выходит за рамки ISMS. Организация может иметь несколько ISMS в пределах своих границ. Таким образом руководящий орган может осуществлять общее управление несколькими ISMS. Большая часть этого документа составлена с учетом такого подхода.

Четыре процесса общего управления, описанные в пункте 7.3, остаются актуальными. Однако в зависимости от отношений между организацией (организациями) ISMS и материнским объектом может иметь место одна из следующих ситуаций.

- Каждая организация ISMS функционирует как автономная часть материнского объекта и, следовательно, имеет собственные бизнес-задачи. В этом случае задачи организации ISMS в области информационной безопасности должны быть согласованы с ее бизнес-задачами.
- Каждая организация ISMS отвечает за выполнение одной или нескольких бизнес-задач своего материнского объекта. В этом случае задачи организации ISMS в области информационной безопасности должны быть согласованы с бизнес-задачами ее материнского объекта.

- На каждую организацию ISMS возложена ответственность за управление каким-либо аспектом риска информационной безопасности от имени материнского объекта. В этом случае задачи организации ISMS в области информационной безопасности должны быть определены материнским объектом, что обеспечит соответствие его бизнес-задачам.

Также существует взаимосвязь между высшим руководством каждой организации ISMS и руководящим органом материнского объекта. Высшее руководство и руководящий орган могут иметь один и тот же состав, иметь несколько общих членов или не иметь ни одного общего члена. Для определения состава руководящего органа и заинтересованных сторон следует использовать рисунок B.1.

8.2.3 Тип C. В состав организации ISMS входят подразделения нескольких объектов

В данной ситуации организация ISMS управляется и контролируется высшим руководством как обычно, но охватывает несколько объектов. Это наблюдается в том случае, если более крупный объект управляет группой объектов с общим контекстом информационной безопасности и общими требованиями к поднабору решаемых задач, например когда для предоставления услуг собираются, обрабатываются, хранятся и используются личные данные. Несколько руководящих органов также могут использовать одну ISMS; например, организация может предоставлять ISMS в качестве услуги многим клиентам.

В том случае, когда в состав организации ISMS входят подразделения нескольких объектов:

- процессы общего управления, описанные в пункте 7.3, остаются неизменными;
- задачи организации ISMS в области информационной безопасности должны быть согласованы с общими бизнес-задачами участвующих объектов.

Приложение A

Взаимосвязь между процессами общего управления

(Данное Приложение не является неотъемлемой частью настоящей Рекомендации | Международного стандарта.)

На рисунке A.1 показана взаимосвязь между общим процессом управления информационной безопасностью и общим процессом управления информационными технологиями.

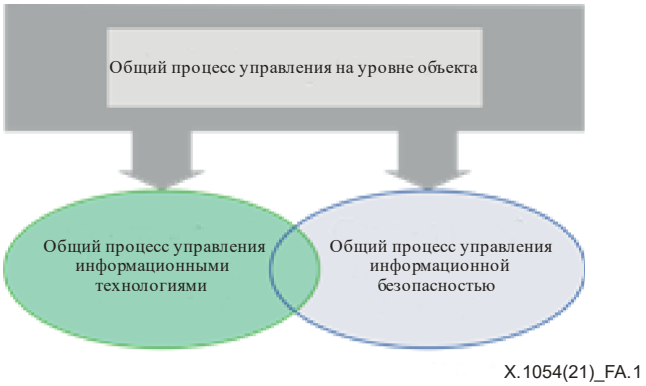

Рисунок A.1 – Взаимосвязь между общим процессом управления информационной безопасностью и общим процессом управления информационными технологиями

Общая сфера охвата общего процесса управления информационными технологиями направлена на ресурсы, требуемые для приобретения, обработки, хранения и распространения информации, тогда как в сферу охвата общего процесса управления информационной безопасностью входит обеспечение конфиденциальности, целостности и доступности информации. В обеих схемах общего управления можно применять следующие процессы управления: оценку, руководство, контроль и информирование.

Приложение B

Типы организаций ISMS

(Данное Приложение не является неотъемлемой частью настоящей Рекомендации | Международного стандарта)

Существует три типа взаимосвязей между организацией, управляющей ISMS, и объектом, применяющим ISMS. Эти взаимосвязи также оказывают влияние на состав высшего руководства ISMS и руководящего органа объекта. Приводимый ниже перечень и рисунок B.1 иллюстрируют эти типы взаимосвязей.

Тип A. Объект и организация ISMS совпадают.

- Руководящий орган тот же, что и высшее руководство ISMS.

Тип B. Организация ISMS входит в состав объекта (причем в рамках этого объекта могут функционировать несколько ISMS).

- В состав руководящего органа могут входить некоторые члены высшего руководства каждой ISMS, но полного совпадения нет.

Тип C. Одна ISMS на несколько объектов.

- Если объекты непосредственно заинтересованы в ISMS, то руководящий орган каждого такого объекта может иметь своих членов в высшем руководстве ISMS.
- Когда ISMS предоставляется третьей стороной в качестве услуги, в состав высшего руководства ISMS редко входят члены руководящих органов объектов, совместно использующих ISMS.

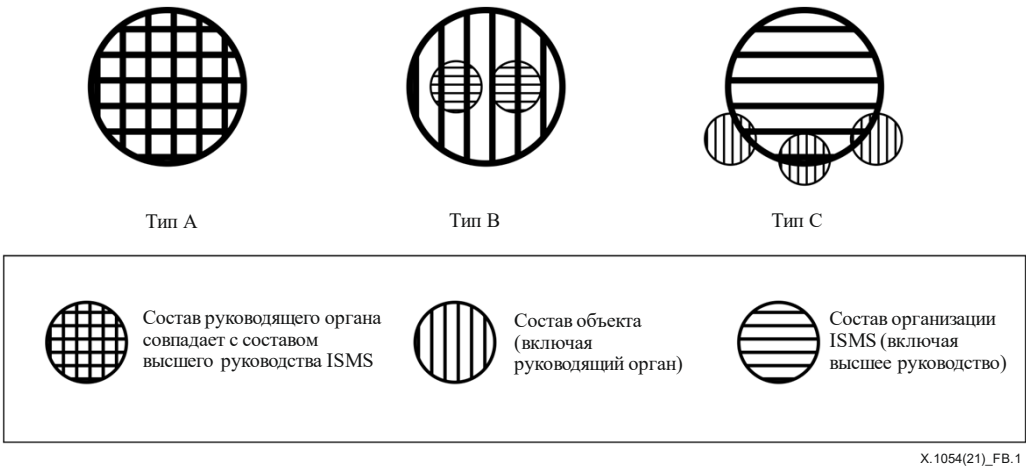

Рисунок B.1 – Возможные взаимосвязи между объектом (объектами) и его (их) ISMS

Приложение C

Примеры информирования

(Данное Приложение не является неотъемлемой частью настоящей Рекомендации | Международного стандарта.)

Один из примеров информирования можно наблюдать на фондовых рынках, где компании обязаны раскрывать риски информационной безопасности по закону или отраслевому регламенту. Другим примером служит отчет об экологической и социальной ответственности и общем управлении (ESG) как средство для организации объяснить/сообщить заинтересованным сторонам о своей деятельности в экологической, социальной и экономической сферах. В некоторых отчетах ESG описывается подход организации к защите конфиденциальных данных, деятельность по обеспечению информационной безопасности и кризисное управление для предотвращения инцидентов, связанных с безопасностью.

В деятельности по разработке методов информирования также следует учитывать непредвиденные последствия недопонимания аудиторией или неправильных выводов, а также попадания информации к людям, не относящимся к целевой аудитории.

Библиография

[1] Recommendation ITU-T X.1051 (2016) | ISO/IEC 27011:2016, *Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations.*

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

[3] ISO 37001:2016, *Anti-bribery management systems – Requirements with guidance for use.*

[4] ISO/IEC 9001:2015, *Quality management systems – Requirements.*

[5] ISO/IEC 27000:2018, *Information security, cybersecurity and privacy protection – Overview and vocabulary.*

[6] ISO/IEC 27002:2013, *Information security, cybersecurity and privacy protection – Code of practice for information security controls.*

[7] ISO/IEC 38500:2015, *Information technology – Governance of IT for the organization.*

[8] ISO Guide 73:2009.

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

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

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

[12] 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.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Принципы тарификации и учета и экономические и стратегические вопросы международной электросвязи/ИКТ
Серия E	Общая эксплуатация сети, телефонная служба, функционирование служб и человеческие факторы
Серия F	Нетелефонные службы электросвязи
Серия G	Системы и среда передачи, цифровые системы и сети
Серия H	Аудиовизуальные и мультимедийные системы
Серия I	Цифровая сеть с интеграцией служб
Серия J	Кабельные сети и передача сигналов телевизионных и звуковых программ и других мультимедийных сигналов
Серия K	Защита от помех
Серия L	Окружающая среда и ИКТ, изменение климата, электронные отходы, энергоэффективность; конструкция, прокладка и защита кабелей и других элементов линейно-кабельных сооружений
Серия M	Управление электросвязью, включая СУЭ и техническое обслуживание сетей
Серия N	Техническое обслуживание: международные каналы передачи звуковых и телевизионных программ
Серия O	Требования к измерительной аппаратуре
Серия P	Качество телефонной передачи, телефонные установки, сети местных линий
Серия Q	Коммутация и сигнализация, а также соответствующие измерения и испытания
Серия R	Телеграфная передача
Серия S	Оконечное оборудование для телеграфных служб
Серия T	Оконечное оборудование для телематических служб
Серия U	Телеграфная коммутация
Серия V	Передача данных по телефонной сети
Серия X	**Сети передачи данных, взаимосвязь открытых систем и безопасность**
Серия Y	Глобальная информационная инфраструктура, аспекты протокола Интернет, сети последующих поколений, интернет вещей и умные города
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2022 г.