Международный союз электросвязи

МСЭ-Т X.1054

СЕКТОР СТАНДАРТИЗАЦИИ
ЭЛЕКТРОСВЯЗИ МСЭ

(09/2012)

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

Безопасность информации и сетей – Управление безопасностью

Информационная технология – Методы обеспечения безопасности – Общий процесс управления информационной безопасностью

Рекомендация МСЭ-Т X.1054

ITU-T

Международный союз электросвязи

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	
Безопасность многоадресной передачи	X.1100–X.1109
Безопасность домашних сетей	X.1110–X.1119
Безопасность подвижной связи	X.1120–X.1139
Безопасность веб-среды	X.1140–X.1149
Протоколы безопасности	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	
Связь в чрезвычайных ситуациях	X.1300–X.1309
Безопасность повсеместных сенсорных сетей	X.1310–X.1339
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

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

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

Информационная технология – Методы обеспечения безопасности – 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.

Информационная безопасность стала для организаций одним из важнейших вопросов. Это связано не только с расширением регуляторных требований, но и с тем, что недостаточность мер информационной безопасности, принимаемых той или иной организацией, может непосредственно отразиться на ее репутации.

В связи с этим от руководящего органа, в рамках его обязанностей в области управления, все чаще требуется осуществлять надзор за информационной безопасностью, чтобы гарантировать достижение целей организации.

Кроме того, общий процесс управления информационной безопасностью обеспечивает прочную связь между руководящим органом организации, ее исполнительным руководством и сотрудниками, ответственными за реализацию и функционирование системы управления информационной безопасностью.

В Рекомендации представлены необходимые полномочия по стимулированию в рамках всей организации инициатив в области информационной безопасности.

Кроме того, эффективный общий процесс управления информационной безопасностью гарантирует получение руководящим органом надлежащей отчетности, сформулированной в контексте коммерческой деятельности, о деятельности в области информационной безопасности. Это позволит принимать адекватные и своевременные решения по вопросам информационной безопасности, поддерживающие стратегические цели организации.

Хронологическая справка

Издание	Рекомендация	Утверждение	Исследовательская комиссия
1.0	МСЭ-Т X.1054	07.09.2012 г.	17-я

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 с целью 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 извещение 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

МЕЖДУНАРОДНЫЙ СТАНДАРТ
РЕКОМЕНДАЦИЯ МСЭ-Т

Информационная технология – Методы обеспечения безопасности – Общий процесс управления информационной безопасностью

1 Сфера применения

В настоящей Рекомендации | Международном стандарте приводятся концепции и руководство по принципам и процессам общего процесса управления информационной безопасностью, с помощью которых организации могут оценивать, направлять и контролировать управление информационной безопасностью.

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

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 27000:2009, Information Technology − Security techniques – Information security management systems – Overview and vocabulary.

3 Определения

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

3.1 **исполнительное руководство**: Лицо или группа людей, которым руководящий орган передал полномочия по реализации стратегий и направлений политики для достижения целей данной организации.

ПРИМЕЧАНИЕ 1. – Исполнительное руководство относится к части высшего руководства. Для удобства обзора должностных функций в настоящем стандарте различаются две группы в рамках высшего руководства: руководящий орган и исполнительные руководители.

ПРИМЕЧАНИЕ 2. – В состав исполнительного руководства могут входить главные исполнительные директора, главные финансовые директора (CFO), главные операционные директора (COO), руководители информационных служб (CIO), руководители служб информационной безопасности (CISO) и лица с аналогичными должностными функциями.

3.2 **руководящий орган**: Лицо или группа людей, которые несут ответственность за результаты деятельности и согласованность действий данной организации.

ПРИМЕЧАНИЕ. – Руководящий орган составляет часть высшего руководства: Для удобства обзора должностных функций в настоящем стандарте различаются две группы в рамках высшего руководства: руководящий орган и исполнительное руководство.

3.3 **общий процесс управления информационной безопасностью**: Система, с помощью которой обеспечивается руководство связанной с безопасностью деятельностью организации и контроль за такой деятельностью.

3.4 **заинтересованная сторона**: Любые лицо или организация, которые могут влиять на деятельность данной организации, на которых может влиять ее деятельность или которые считают, что на них влияет ее деятельность.

ПРИМЕЧАНИЕ. – Заинтересованной стороной может быть директивный орган.

4 Концепции

4.1 Общие положения

Общий процесс управления информационной безопасностью необходим для согласования задач и стратегий информационной безопасности с задачами и стратегиями коммерческой деятельности, и для него требуется соблюдение законодательства, нормативных положений и контрактов. Его следует оценивать, анализировать и реализовывать с помощью подхода к управлению рисками, обеспечиваемого внутренней системой контроля.

Руководящий орган несет полную ответственность за решения организации и за ее деятельность. В том что касается информационной безопасности, руководящий орган должен обеспечивать эффективность, действенность и приемлемость подхода данной организации к информационной безопасности и, в соответствии с задачами и стратегиями коммерческой деятельности, уделять должное внимание ожиданиям заинтересованных сторон. У разных заинтересованных сторон могут быть различные ценности и потребности.

4.2 Задачи

Задачи общего процесса управления информационной безопасностью состоят в следующем:

- согласование задач и стратегии информационной безопасности с задачами и стратегией коммерческой деятельности (стратегическое согласование);
- обеспечение ценности для руководящего органа и заинтересованных сторон (обеспечение ценности);
- обеспечение адекватного рассмотрения информационных рисков (подотчетность).

4.3 Желаемые результаты

Желаемые результаты эффективного внедрения общего процесса управления информационной безопасностью включают:

- понимание руководящим органом статуса информационной безопасности;
- динамичный подход к принятию решений по поводу информационных рисков;
- эффективные и действенные инвестиции в информационную безопасность;
- соответствие внешним требованиям (правовым, регуляторным или договорным).

4.4 Взаимосвязь

В рамках той или иной организации имеются несколько других моделей областей управления, такие как управление информационными технологиями и организационное управление. Каждая модель управления является неотъемлемой составляющей общего процесса управления организацией, в котором подчеркивается важность согласования с задачами коммерческой деятельности. Как правило, целесообразно, чтобы руководящий орган разработал целостную и единую картину своей модели управления, частью которой должен быть общий процесс управления информационной безопасностью. Сферы охвата моделей управления иногда пересекаются. Например, взаимосвязь между общим процессом управления информационной безопасностью и общим процессом управления информационными технологиями показана на рисунке 1.

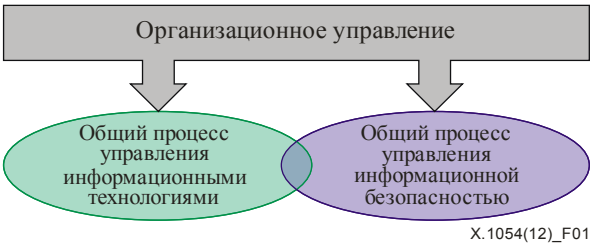

Рисунок 1 – Взаимосвязь между общим процессом управления информационной безопасностью и общим процессом управления информационными технологиями

При этом общая сфера охвата общего процесса управления информационными технологиями направлена на те ресурсы, которые требуются для приобретения, обработки, хранения и распространения информации. А в сферу охвата общего процесса управления информационной безопасностью входит обеспечение конфиденциальности, целостности и наличия информации. К обеим схемам управления необходимо применять следующие процессы управления: EDM (оценка, руководство, контроль). Вместе с тем общему процессу управления информационной безопасностью требуется дополнительный внутренний процесс – "информирование".

В пункте 5 описаны задачи, для которых от руководящего органа требуется внедрить общий процесс управления информационной безопасностью. Задачи управления также связаны с требованиями к управлению, указанными в ИСО/МЭК 27001, а также в других стандартах в сфере ISMS, ссылки на которые приводятся в библиографии.

5 Принципы и процессы

5.1 Обзор

В данном пункте описываются принципы и процессы, которые образуют вместе общий процесс управления информационной безопасностью. Принципы общего процесса управления информационной безопасностью являются признанными нормами деятельности или поведения в сфере управления, которые действуют в качестве руководства по внедрению общего процесса управления. Общий процесс управления информационной безопасностью описывает серию задач, которые дают возможность общего процесса управления информационной безопасностью, и взаимосвязи между ними. Он также показывает связь между общим процессом управления и управлением информационной безопасностью. Эти два компонента объясняются в следующих пунктах.

5.2 Принципы

Удовлетворение потребностей заинтересованных сторон и обеспечение ценности для каждой из них являются неотъемлемой частью долгосрочного успеха информационной безопасности. Для выполнения задачи общего процесса управления, которая состоит в тесном согласовании информационной безопасности с целями коммерческой деятельности и в обеспечении ценности для заинтересованных сторон, в данном пункте устанавливаются шесть принципов, ориентированных на действия.

Эти принципы обеспечивают прочную основу для внедрения общего процесса управления информационной безопасностью. Изложение каждого принципа относится к тому, что должно произойти, но не описывается, каким именно образом, когда и кем эти принципы будут внедряться, поскольку эти аспекты зависят от характера организации, внедряющей такие принципы. Руководящему органу следует требовать, чтобы эти принципы применялись, и назначить то или иное лицо, которое будет отвечать за их внедрение, отчитываться об этом и иметь соответствующие полномочия.

Принцип 1: Внедрение информационной безопасности на уровне всей организации

Общий процесс управления информационной безопасностью должен обеспечивать, чтобы деятельность в области информационной безопасности была всесторонней и комплексной. Информационной безопасностью следует заниматься на уровне организации, а при принятии решений следует учитывать интересы коммерческой деятельности, информационной безопасности и все соответствующие аспекты. Деятельность, касающуюся физической и логической безопасности, следует тесно координировать.

Для внедрения безопасности на уровне всей организации необходимо ввести ответственность и подотчетность за информационную безопасность по всем направлениям деятельности организации. Периодически это выходит за обычно понимаемые "границы" деятельности организации, например, когда информация хранится или передается внешними сторонами.

Принцип 2: Принятие подхода, основанного на оценке рисков

Общий процесс управления информационной безопасностью должен основываться на решениях, принимаемых на основе оценки рисков. Определение приемлемой степени безопасности должно основываться на склонности организации к риску, включая утрату конкурентных преимуществ, риски в области соответствия и ответственности, перебои в работе, ущерб репутации и финансовые потери.

Для принятия информации, которая подходит для данной организации, следует, чтобы такое управление соответствовало общему подходу организации к управлению рисками и было в него включено. Приемлемые уровни информационной безопасности следует определить на основе готовности организации к принятию риска, включающего потерю конкурентного преимущества, риски ответственности за исполнение, нарушения деятельности, ущерб для репутации и финансовые потери. Руководящему органу следует выделить соответствующие ресурсы для внедрения управления информационными рисками.

Принцип 3: Установление направленности инвестиционных решений

В общем процессе управления информационной безопасностью должна быть установлена инвестиционная стратегия для обеспечения информационной безопасности на основе достигнутых деловых результатов, что приведет к согласованию требований в области коммерческой деятельности и информационной безопасности в краткосрочной и долгосрочной перспективе, и, таким образом, к удовлетворению текущих и появляющихся потребностей заинтересованных сторон.

Для оптимизации инвестиций в информационную безопасность в целях обеспечения выполнения задач организации, руководящему органу следует обеспечить, чтобы вопрос информационной безопасности был включен в существующие в организации процессы в связи с капитальными и эксплуатационными расходами, соответствием правовым и регуляторным требованиям и отчетностью о рисках.

Принцип 4: Обеспечение соответствия внутренним и внешним требованиям

Общий процесс управления информационной безопасностью должен обеспечивать, чтобы политика и практика в сфере информационной безопасности соответствовали надлежащим обязательным к исполнению законодательству и нормативным положениям, а также принятым коммерческим и договорным условиям и другим внешним или внутренним требованиям.

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

Принцип 5: Содействие созданию среды, благоприятной для безопасности

Общий процесс управления информационной безопасностью должен быть основан на поведении людей, 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 противоречить друг другу, что приведет к невыполнению задач в коммерческой сфере. Следовательно, очень важны согласование и совместные действия различных заинтересованных сторон.

Для создания культуры позитивного отношения к информационной безопасности следует, чтобы руководящий орган требовал и содействовал координации деятельности заинтересованных сторон, а также поддерживал такую координацию в целях согласованного руководства информационной безопасностью. Это обеспечит разработку программ по обучению, профессиональной подготовке и повышению информированности в сфере безопасности.

Принцип 6: Рассмотрение деятельности в связи с коммерческими результатами

Общий процесс управления информационной безопасностью должен обеспечить соответствие подхода, принятого для защиты информации, целям обеспечения работы организации, предоставляя согласованные уровни информационной безопасности. Работу по безопасности следует поддерживать на уровнях, которые необходимы для выполнения нынешних и будущих требований коммерческой деятельности.

Для рассмотрения результативности информационной безопасности с точки зрения общего процесса управления руководящему органу следует оценить такую результативность в отношении ее воздействия на коммерческую деятельность, а не только эффективность и действенность контроля безопасности. Это можно выполнить путем проведения обязательных обзоров программ измерения результативности, аудита и совершенствования деятельности, увязывая таким образом деятельность в сфере информационной безопасности с результатами коммерческой деятельности.

5.3 Процессы

5.3.1 Обзор

Для реализации общего процесса управления информационной безопасностью руководящий орган осуществляет процессы "оценки", "руководства", "контроля" и "информирования". Кроме того, процесс "заверения" обеспечивает независимое и объективное мнение по поводу общего процесса управления информационной безопасностью и достигнутого уровня такой безопасности. На рисунке 2 показана связь между этими процессами.

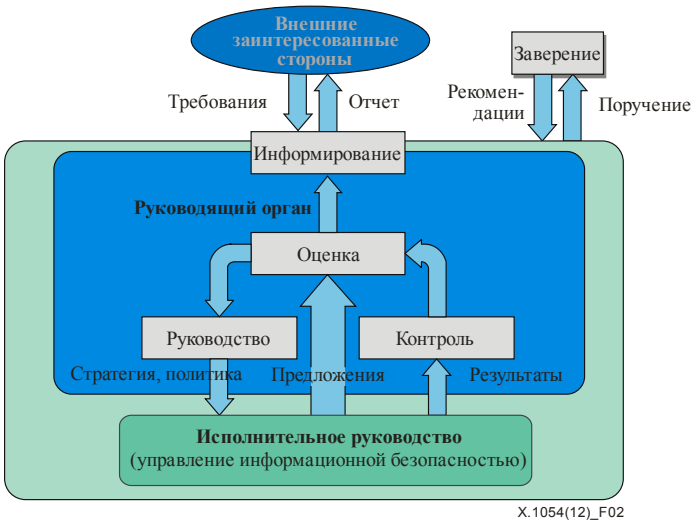

Рисунок 2 – Модель реализации общего процесса управления информационной безопасностью

5.3.2 Оценка

"Оценка" – это общий процесс управления, при котором рассматриваются нынешние и прогнозируемые достижения задач безопасности на основе текущих процессов и запланированных изменений, а также определяется, требуются ли какие-нибудь корректировки для оптимизации достижения стратегических задач в будущем.

Для осуществления процесса "оценки" руководящему органу следует:

- обеспечивать, чтобы в коммерческих инициативах учитывались вопросы информационной безопасности;
- реагировать на результаты деятельности в области информационной безопасности, определять приоритеты действий и инициировать требуемые действия.

Для облегчения процесса "оценки" исполнительному руководству следует:

- обеспечивать, чтобы информационная безопасность адекватным образом поддерживала и подкрепляла задачи коммерческой деятельности;
- представлять руководящему органу новые проекты в области информационной безопасности, которые окажут существенное воздействие.

5.3.3 Руководство

"Руководство" – это общий процесс управления, с помощью которого руководящий орган дает распоряжения по поводу задач в области информационной безопасности и стратегии, которую необходимо реализовывать. 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:

- определять склонность организации к риску;
- утверждать стратегию и политику в области информационной безопасности;
- выделять необходимые инвестиции и ресурсы.

Для облегчения процесса "руководства" исполнительному руководству следует:

- разрабатывать и внедрять стратегию и политику в области информационной безопасности;
- согласовывать задачи в области информационной безопасности с задачами в области коммерческой деятельности;
- содействовать внедрению культуры, благоприятной для информационной безопасности.

5.3.4 Контроль

"Контроль" − это общий процесс управления, который дает руководящему органу возможность оценивать достижение стратегических задач.

Для осуществления процесса "контроля" руководящему органу следует:

- оценивать эффективность деятельности по управлению информационной безопасностью;
- обеспечивать соответствие внутренним и внешним требованиям;
- рассматривать вопросы, связанные с изменением коммерческой деятельности, правовой и регуляторной средой и их потенциальным воздействием на информационные риски.

Для облегчения процесса "контроля" исполнительному руководству следует:

- выбирать подходящие, с точки зрения коммерческой деятельности, показатели работы;
- обеспечивать, чтобы руководящему органу сообщалось о результатах деятельности в области информационной безопасности, в том числе о результатах деятельности, ранее определенной руководящим органом, и о ее воздействии на организацию;
- предупреждать руководящий орган о новых событиях, сказывающихся на информационных рисках и информационной безопасности.

5.3.5 Информирование

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

Одним из методов "информирования" является статус информационной безопасности, который объясняет для заинтересованных сторон деятельность и вопросы в области информационной безопасности. Соответствующие примеры приводятся в Приложениях A и B.

Для осуществления процесса "информирования" руководящему органу следует:

- сообщать внешним заинтересованным сторонам о том, что данная организация применяет уровень информационной безопасности, который соответствует характеру ее коммерческой деятельности;
- уведомлять исполнительное руководство о результатах любых внешних обзоров, в ходе которых были определены вопросы в области информационной безопасности, и поручать выполнять коррективные меры;
- распознавать информацию, касающуюся регуляторных обязательств, ожиданий заинтересованных сторон и коммерческих потребностей в отношении информационной безопасности.

Для облегчения процесса "информирования" исполнительному руководству следует:

- сообщать руководящему органу о любых вопросах, которые требуют его внимания и, возможно, решения;
- инструктировать соответствующие заинтересованные стороны в отношении подробных мер, которые необходимо принимать для обеспечения выполнения поручений и решений руководящего органа.

5.3.6 Заверение

"Заверение" − это общий процесс управления, с помощью которого руководящий орган поручает проводить независимые и объективные аудит, обзоры или сертификации. Эти меры обеспечат определение и проверку задач и действий, связанных с осуществлением руководящей деятельности и проведением операций в целях достижения желаемого уровня информационной безопасности.

Для осуществления процесса "заверения" руководящему органу следует:

- поручать составлять независимые и объективные мнения по поводу того, насколько соблюдаются требования подотчетности в отношении желаемого уровня информационной безопасности.

Для облегчения процесса "заверения" исполнительному руководству следует:

- помогать в проведении аудита, обзоров или сертификаций, порученных руководящим органом.

Приложение A

Пример статуса информационной безопасности

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

Организация может разработать статус информационной безопасности и довести его до сведения заинтересованных сторон в качестве средства сообщать данные для информационной безопасности.

Организации следует выбрать и принять формат и содержание статуса информационной безопасности. В Приложении A представлен пример использования протокола аудита информационной безопасности для заявления об удовлетворенности.

Таблица A — Статус информационной безопасности

Руководство удовлетворено тем, что за период **mmm–nnn** контроль и процедуры в области информационной безопасности, которые основаны на критерии, приведенном в **xyz** (например, серии 27000, COBIT) и касающемся операционных процедур и систем организации, и которые были подтверждены контролем со стороны высшего руководства, осуществлялись с эффективностью, достаточной для того, чтобы дать разумные гарантии в том, что установленные задачи контроля информационной безопасности в связи с конфиденциальностью, целостностью и готовностью, были достигнуты. Руководство предоставило с этой целью компании **ABC**, в качестве внешнего аудитора в области информационной безопасности, письмо-подтверждение. Компания ABC была назначена Советом директоров для изучения заявления руководства по поводу контроля информационной безопасности. Проверка проводилась в соответствии с установленными стандартами и включала оценку проекта, операционной эффективности контроля и процедур информационной безопасности с помощью выборочного тестирования. В связи с этим компания **ABC** опубликовала для руководства мнение о том, что результаты проведенного тестирования показывают, что, за особыми исключениями, основанными на критериях руководства, установленных в **xyz** (например, серии 27000, COBIT), контроль в существенной части был эффективным. Полное письмо-заявление руководства и отчет о внешнем аудите с любыми выявленными исключениями в отношении контроля информационной безопасности обсуждались с Комитетом по аудиту и были представлены всем членам Совета директоров. Копии предоставляются по запросу всем заинтересованным сторонам.

ПРИМЕЧАНИЕ. – "nnn", "mmm", "xyz", "ABC" – поля для заполнения. В фактических протоколах следует указывать конкретные даты и названия.

Приложение B

Пример подробного статуса информационной безопасности

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

В данном Приложении представлен пример статуса информационной безопасности, в котором раскрывается подробное содержание. Это особенно полезно для организаций, которые ожидают улучшить свою репутацию, делая упор на обеспечиваемой ими безопасности, например для предприятий в сфере ИКТ. Прозрачность подхода такой организации к своим рискам безопасности и раскрытие соответствующей информации также являются эффективными способами повышения доверия. С помощью такой деятельности можно добиться того, что у всех заинтересованных сторон будет одинаковый уровень информированности.

Таблица B – Подробный статус информационной безопасности

Введение

- **Сфера применения** (стратегия, политика, стандарты), **охват** (географические/организационные единицы), **охватываемый период** (месяц/квартал/шесть месяцев/год)

Общий статус

- **Удовлетворительный/не вполне удовлетворительный/неудовлетворительный**

Уточненные данные (если это требуется и целесообразно)

- Прогресс в направлении достижения целей стратегии информационной безопасности

  Выполненные элементы/выполняемые элементы/планируемые элементы
- Изменения в системе управления информационной безопасностью

  Пересмотр политики ISMS, организационная структура для внедрения ISMS (включая распределение обязанностей)
- Прогресс в направлении сертификации

  Сертификация (повторная сертификация) ISMS, сертифицированный аудит информационной безопасности
- Составление бюджета/комплектование штатов/профессиональная подготовка

  Финансовая ситуация, достаточный численный состав персонала, квалификации в области информационной безопасности
- Другая деятельность в области информационной безопасности

  Участие управления в бесперебойной деятельности, информационно-пропагандистские кампании, помощь в проведении внутреннего/внешнего аудита

Существенные вопросы (если имеются)

- Результаты обзоров информационной безопасности

  Рекомендации, принимаемые руководством меры, планы действий, целевые сроки
- Прогресс в отношении основных отчетов о внутреннем/внешнем аудите

  Рекомендации, принимаемые руководством меры, планы действий, целевые сроки
- Инциденты в области информационной безопасности

  Оцениваемое воздействие, планы действий, целевые сроки
- Соблюдение (несоблюдение) соответствующего законодательства и нормативных положений

  Оцениваемое воздействие, планы действий, целевые сроки

Необходимое(ые) решение(я) (если есть)

- Дополнительные ресурсы

  Чтобы информационная безопасность могла содействовать коммерческим инициативам

Библиография

[1] Рекомендация МСЭ-Т X.1051 (2008 г.) | ИСО/МЭК 27011:2008, *Информационные технологии – Методы обеспечения безопасности – Руководящие указания по управлению информационной безопасностью для организаций электросвязи, основанные на стандарте ИСО/МЭК 27002*.

[2] ISO/IEC 27001:2005, *Information technology – Security techniques – Requirements of information security management systems*.

[3] ISO/IEC 27002:2005, *Information technology – Security techniques – Code of practice for information security management*.

[4] ISO/IEC 27005:2011, *Information technology – Security techniques – Guidelines for information security risk management*.

[5] ISO/IEC 38500:2008, *Corporate Governance of Information technology – a standard for corporate governance of information technology*.

[6] ITGI, *Information Security Governance framework: 2009*.

[7] ISF, *Standard of Good Practice for Information Security: 2011*.

СЕРИИ РЕКОМЕНДАЦИЙ МСЭ-Т

Серия A	Организация работы МСЭ-Т
Серия D	Общие принципы тарификации
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	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	Оконечное оборудование, субъективные и объективные методы оценки
Серия Q	Коммутация и сигнализация
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 и сети последующих поколений
Серия Z	Языки и общие аспекты программного обеспечения для систем электросвязи

Отпечатано в Швейцарии
Женева, 2013 г.