ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27036-1— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Информационная безопасность во взаимоотношениях с поставщиками

Часть 1

Обзор и основные понятия

(ISO/IEC 27036-1:2014, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН); Акционерным обществом «Научно-производственное объединение «Эшелон» (АО «НПО Эшелон») и Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО ИАВЦ) на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 20 мая 2021 г. № 418-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27036-1:2014 «Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 1. Обзор и основные понятия» (ISO/IEC 27036-1:2014 «Information technology. Security techniques. Information security for supplier relationships. Part 1: Overview and concepts», IDT).

ИСО/МЭК 27036-1 разработан подкомитетом ПК 27 «Методы и средства обеспечения безопасности ИТ» Совместного технического комитета СТК 1 «Информационные технологии» Международной организации по стандартизации (ИСО) и Международной электротехнической комиссии (МЭК).

При применении настоящего стандарта рекомендуется использовать вместо ссылочного международного стандарта соответствующий ему национальный стандарт, сведения о котором приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые положения международного стандарта, указанного в пункте 4, могут являться объектом патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут ответственности за идентификацию подобных патентных прав

Правила применения настоящего стандарта установлены в статье 26 Федерального закона от 29 июня 2015 г. № 162-ФЗ «О стандартизации в Российской Федерации». Информация об изменениях к настоящему стандарту публикуется в ежегодном (по состоянию на 1 января текущего года) информационном указателе «Национальные стандарты», а официальный текст изменений и поправок — в ежемесячном информационном указателе «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ближайшем выпуске ежемесячного информационного указателя «Национальные стандарты». Соответствующая информация, уведомление и тексты размещаются также в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет (www.gost.ru)

Содержание

Введение

Серия ИСО/МЭК 27036 состоит из следующих частей под общим названием «Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками».

- часть 1. Обзор и основные понятия;
- часть 2. Требования;
- часть 3. Рекомендации по обеспечению безопасности цепи поставок информационных и коммуникационных технологий;
- часть 4. Рекомендации по обеспечению безопасности облачных услуг.

Большинство (если не все) организации во всем мире, независимо от их размера или ключевых сфер деятельности, взаимодействуют с различными видами поставщиков продукции и услуг.

Такие поставщики могут иметь или прямой, или косвенный доступ к информации и информационным системам приобретающей стороны, либо предоставлять элементы (программное обеспечение, аппаратные средства, процессы или человеческие ресурсы), которые будут задействованы в процессе обработки информации. У приобретающей стороны может также быть физический и/или логический доступ к информации поставщика, когда они осуществляют мониторинг или контролируют процессы производства и поставки от поставщика.

Таким образом, приобретающая сторона и поставщики могут являться друг для друга источником рисков в области информационной безопасности. Эти риски должны оцениваться и рассматриваться как организациями-получателями, так и организациями-поставщиками посредством надлежащего управления информационной безопасностью и реализацией соответствующих мер защиты информации. В большинстве случаев организации принимали международные стандарты ИСО/МЭК 27001 и/или ИСО/МЭК 27002 для управления своей информационной безопасностью. Эти международные стандарты должны также быть приняты при управлении в отношениях с поставщиками для осуществления эффективного контроля рисков в области информационной безопасности, свойственных этим отношениям.

Настоящий стандарт содержит дополнительные подробные указания по реализации мер защиты информации, касающихся отношений с поставщиками, которые описаны в ИСО/МЭК 27002 в качестве общих рекомендаций[1)].

Отношения с поставщиками в контексте настоящего стандарта включают в себя любое отношение с поставщиком, которое может иметь последствия для информационной безопасности, например, информационные технологии, медицинские услуги, услуги по уборке помещений, консультационные услуги, партнерские отношения в области НИОКР (R&D), аутсорсинговые приложения или услуги облачных вычислений (такие как программное обеспечение, платформа или инфраструктура как услуга).

Как поставщик, так и приобретающая сторона должны нести равную ответственность чтобы достичь поставленных целей в отношениях поставщика с приобретающей стороной и адекватно реагировать на риски в области информационной безопасности, которые могут возникнуть. Ожидается, что обе стороны будут выполнять требования и инструкции настоящего стандарта. Кроме того, для поддержания отношений поставщика с приобретающей стороной должны быть реализованы основные процессы (например, управление, управление бизнесом, оперативное управление и управление персоналом). Эти процессы обеспечат поддержку с точки зрения информационной безопасности, а также достижение бизнес-целей.

[1)] Положения настоящего стандарта должны рассматриваться с учетом требований национальных нормативных правовых актов и стандартов Российской Федерации в области защиты информации.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Информационная безопасность во взаимоотношениях с поставщиками

Часть 1

Обзор и основные понятия

Information technology. Security techniques. Information security for supplier relationships.
Part 1. Overview and concepts

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт является вводной частью ИСО/МЭК 27036. В ней содержится обзор руководящих положений, призванных помочь организациям в обеспечении безопасности их информации и информационных систем в контексте отношений с поставщиками. В настоящем стандарте также вводятся понятия, которые подробно описаны в других частях ИСО/МЭК 27036. В настоящем стандарте рассматриваются возможности как приобретающей стороны, так и поставщиков.

2 Нормативные ссылки

В настоящем стандарте использована нормативная ссылка на следующий стандарт. Для датированной ссылки применяют только указанное издание ссылочного стандарта, для недатированной — 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)

3 Термины и определения

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

3.1

приобретающая сторона (acquirer): Заинтересованная сторона, которая приобретает у поставщика продукт или услугу.

Примечание — Приобретение может включить или не включать обмен денежными средствами.

[ИСО/МЭК 15288:2008, 4.1, изменено — Исходное примечание было удалено, слово «получает», было удалено из определения, и было добавлено примечание]

3.2

приобретение (acquisition): Процесс получения продукта или услуги.
[ИСО/МЭК 15288:2008, 4.2, изменено — слово «система», было удалено]

3.3

соглашение (agreement): Обоюдное подтверждение сроков и условий, согласно которым осуществляются рабочие отношения.
[ИСО/МЭК 15288:2008, 4.4]

3.4

жизненный цикл (life cycle): Развитие системы, продукта, услуги, проекта или иного рукотворного объекта от стадии замысла до момента прекращения его использования.
[ИСО/МЭК 15288:2008, 4.11]

3.5

фаза постконтроля (downstream): Погрузочно-разгрузочные работы, процессы и перемещение, когда продукты и услуги в цепи поставок находятся вне сферы контроля этой организации.
[ИСО 28001:2007, 3.10, изменено — слово «товары» было заменено на «продукты и услуги» с целью заострить внимание на данном определении]

3.6 **аутсорсинг** (outsourcing): Приобретение услуг (с или без продуктов) в поддержку бизнес-функции для осуществления деятельности с использованием ресурсов поставщика, а не приобретающей стороны.

3.7

процесс (process): Совокупность взаимосвязанных или взаимодействующих видов деятельности, преобразующих входы в выходы.
[ИСО 9000:2005, 3.4.1, изменено — примечания были удалены]

3.8 **заинтересованная сторона** (stakeholder): Физическое лицо или организация, заинтересованные в активах при отношениях с поставщиком.

Примечание — В целях настоящего стандарта актив является информацией, связанной с продуктами и услугами.

3.9

поставщик (supplier): Организация или физическое лицо, которое заключает соглашение с приобретающей стороной по предоставлению продукта или услуги.

Примечания

1 Другими терминами, обычно используемыми для обозначения поставщика являются: подрядчик, производитель, торговец или продавец.

2 Приобретающая сторона и поставщик могут являться частью одной и той же организации.

3 Типы поставщиков включают в себя те организации, которые допускают заключение соглашений с приобретающей стороной и те, которые этого не допускают. Например, таких как пользовательское соглашение, условия использования, или использование продуктов с открытым исходным кодом, защищенных авторским правом или результатов интеллектуальной деятельности.

[ИСО/МЭК 15288:2008, 4.30, изменено — Добавлено примечание 3]

3.10 **взаимоотношение с поставщиком** (supplier relationship): Одно соглашение или несколько соглашений между приобретающей стороной и поставщиками о ведении бизнеса, поставке продуктов или услуг и получении коммерческой выгоды.

3.11

цепь поставок (supply chain): Совокупность организаций со взаимосвязанным набором ресурсов и процессов, каждая из которых выступает в качестве приобретающей стороны, поставщика или одновременно в качестве обеих сторон, для формирования последовательных отношений с поставщиками, установленных при размещении заказа на поставку, заключения договора или другого официального контракта на поставку.

Примечания

1 Цепь поставок может включать в себя продавцов, производственное оборудование, логистических провайдеров, внутренние распределительные центры, дистрибьюторов, оптовиков и другие организации, участвующие в производстве, обработке, транспортировке и доставке грузов и связанных с ними услуг.

2 Вид цепи поставок рассматривается с позиции приобретающей стороны.

[ИСО 28001:2007, 3.24, изменено — определение было изменено, чтобы в большей степени сфокусироваться на организации и отношениях; Было добавлено примечание 2]

3.12

система (system): Комбинация взаимодействующих элементов, упорядоченных для достижения одной или нескольких поставленных целей.

Примечания

1 Систему можно рассматривать как продукт или как предоставляемые ею услуги.

2 На практике интерпретация данного термина зачастую уточняется с помощью ассоциативного существительного, например система самолета. В некоторых случаях слово система может заменяться контекстно-зависимым синонимом, например самолет, хотя это может впоследствии затруднить восприятие системных принципов.

[ИСО/МЭК 15288:2008, 4.31]

3.13

доверие (trust): Отношения между двумя организациями и/или элементами, состоящие из ряда операций и политики безопасности, в которых элемент «x» доверяет элементу «y», если и только если «x» уверен, что «y» будет вести себя определенным образом (по отношению к операциям), не нарушающим данную политику безопасности.

[ИСО/МЭК 13888-1:2009, 3.59, изменено — примечание было удалено]

3.14

фаза предконтроля (upstream): Транспортировка, процессы и перемещение продукции и услуг, имеющих место до того, как организация принимает продукции и услуги под свой контроль в цепи поставок.

[ISO 28001:2007, 3.27, изменено — слово «товары» было заменено на «продукции и услуги» с целью заострить внимание на данном изменении]

3.15 **прозрачность** (visibility): Свойство системы или процесса, которое позволяет системным элементам и процессам быть задокументированными и доступными для мониторинга и контроля.

4 Сокращения

В настоящем стандарте применены следующие сокращения:

BPaaS — бизнес-процесс как услуга;

IaaS — инфраструктура как услуга;

ИКТ — информационно-коммуникационные технологии;

PaaS — платформа как услуга;

НИОКР — научно-исследовательские и опытно-конструкторские работы;

SaaS — программное обеспечение как услуга.

5 Определение проблемы и ключевые понятия

5.1 Мотивы установления отношений с поставщиками

Организации часто принимают решение о формировании и/или сохранении отношений с поставщиками исходя из множества бизнес-причин для того, чтобы воспользоваться преимуществами, которые они могут предоставить. Ниже вкратце изложены потенциальные мотивы для установления отношений с поставщиком:

a) сосредоточение внутренних ресурсов на основных бизнес-функциях, что может привести к сокращению затрат и повышению дохода от инвестиций (например, аутсорсинг услуг ИКТ);

b) приобретение краткосрочной или узкоспециализированной компетенции, которой организация еще не обладает (например, нанимая рекламную фирму) для достижения определенных бизнес-целей;

c) приобретение коммунальных или базовых услуг, которые являются общими или легкодоступными (например, электроэнергия и телекоммуникации) и которые не могут быть эффективно предоставлены организацией;

d) обеспечение возможности осуществления предпринимательской деятельности в другом географическом месте;

e) приобретение новых или заменяющих ИКТ продуктов или услуг (например, ноутбуков, принтеров, серверов, маршрутизаторов, программных приложений, емкости запоминающих устройств, сетевых подключений, услуг управления ИКТ и т. д.), которые обеспечивают производительность рабочей силы и другие потребности бизнеса в вычислениях.

Поставщики могут предоставлять множество продуктов или услуг, включая ИТ-аутсорсинг, профессиональные услуги, основные коммунальные услуги (техобслуживание оборудования, услуги охраны, услуги по уборке и доставке и т. д.), облачные вычислительные услуги, информационно-коммуникационные технологии (ИКТ), управление знаниями, НИОКР, производство, логистику, медицинское обслуживание, интернет-услуги и многие другие.

5.2 Виды взаимоотношений с поставщиками

5.2.1 Взаимоотношения с поставщиками продукции

Когда приобретающая сторона вступает во взаимоотношения с поставщиком продукции, она зачастую приобретает продукты с заранее оговоренными спецификациями и сроком поставки для производства собственной продукции.

У поставщика может быть доступ к информации приобретающей стороны при поставке и поддержке продукта, что в результате может привести к возникновению рисков в области информационной безопасности в отношении информации приобретающей стороны. Невыполнение требований, уязвимости в программном обеспечении и сбои в работе продуктов, а также непреднамеренное раскрытие конфиденциальной информации также могут привести к возникновению рисков в области информационной безопасности приобретающей стороны.

Для управления этими рисками в области информационной безопасности приобретающая сторона может устанавливать правила доступа поставщика к своей информации. Приобретающая сторона может также пожелать контролировать элементы производственных процессов поставщика для поддержания качества продукции и снижения рисков в области информационной безопасности, связанных с уязвимостями, неисправностями или другими нарушениями требований. Это, в свою очередь, может представлять угрозу безопасности информации для поставщика, поскольку приобретающая сторона может иметь доступ к информации поставщика в ходе управлении элементами процессов поставщика.

Кроме того, приобретающая сторона может запросить гарантии в отношении спецификации продукции путем мониторинга или аудита производственных процессов или потребовать от поставщика пройти независимую сертификацию для подтверждения наличия надлежащей практики и требуемых процессов. Данные гарантии должны быть заранее согласованы между сторонами.

5.2.2 Взаимоотношения с поставщиками услуг

Когда приобретающая сторона заказывает услуги, поставщик, как правило, имеет доступ к информации покупателя. Это создает потенциальные риски в области информационной безопасности для приобретающей стороны. В случае аутсорсинга бизнес-процессов, например маркетинга, работы колл-центра или инфраструктуры ИКТ организации, значительная часть критически важной бизнес-информации приобретающей стороны может быть передана под управление поставщика. Другие же виды

услуг, как правило, имеют ограниченный доступ к информации приобретающей стороны, например, такие виды услуг, как услуги по питанию и уборке помещений.

Для предоставления некоторых услуг требуется, чтобы информация приобретающей стороны находилась в пределах его объектов, зданий и была доступна поставщику как локально, так и удаленно. Или, например, в других случаях информация приобретающей стороны размещается на сайте поставщика. Эти особые условия могут повлиять на выбор средств мер защиты информации, применимых к приобретающей стороне или поставщику. Примеры того, как расположение может повлиять на доступ поставщика к информации приобретающей стороны, представлены в таблице 2.

Приобретая услуги, заказчики должны установить правила по контролю доступа поставщика к информации приобретающей стороны. Также они могут пожелать контролировать качество услуги для снижения рисков в области информационной безопасности, включая возможность со временем отвечать требованиям по удовлетворению потребностей доступности. Соглашение об уровне обслуживания — это общий способ согласования качества обслуживания. Для поставщика данное соглашение может являться инструментом для того, чтобы ознакомить приобретающую сторону с тем, как он будет удовлетворять ее требованиям качества.

Приобретающая сторона может пожелать получить гарантии в отношении качества услуг путем мониторинга или аудита процессов предоставления услуг поставщиком или потребовать от поставщика пройти независимую сертификацию для подтверждения наличия надлежащей практики и требуемых процессов. Данные гарантии должны быть заранее согласованы между сторонами.

5.2.3 Цепь поставок ИКТ

Цепь поставок ИКТ представляет собой совокупность организаций со связанным набором ресурсов и процессов, которые формируют последовательные отношения поставщиков продукции и услуг ИКТ. Продукт или услуга ИКТ могут состоять из компонентов, ресурсов и процессов, производимых поставщиком, которые могут полностью или частично быть произведены другим поставщиком. Таким образом, все необходимые услуги ИКТ могут предоставляться несколькими поставщиками. Как показано на рисунке 1, организация в цепи поставок ИКТ является приобретающей стороной на фазе постконтроля и поставщиком на фазе предконтроля. Организацию на фазе постконтроля, расположенную рядом, часто называют заказчиком с точки зрения организации, которая предоставляет ей продукты или услуги. Заказчик в конце цепи поставок ИКТ является конечным заказчиком или потребителем. Как правило, конечный заказчик имеет ограниченный контроль над требованиями к информационной безопасности своего непосредственного поставщика и не имеет контроля над требованиями к информационной безопасности за рамками непосредственно прямого поставщика.

Рисунок 1 — Взаимоотношения с поставщиками услуг

Приобретающие стороны и поставщики по всей цепи поставок ИКТ наследуют риски в области информационной безопасности, связанные с отношениями отдельных поставщиков продукции и услуг (см. 5.2.1 и 5.2.2). Однако приобретающей стороне сложно управлять этими рисками в области информационной безопасности посредством передачи, мониторинга и обеспечения своей информационной безопасности по всей цепи поставок ИКТ из-за ограниченной прозрачности и ограниченного доступа к поставщикам своих поставщиков.

5.2.4 Облачные вычисления

Облачные вычисления являются формой отношений с поставщиками, в которых услуга облачных вычислений в целом может быть получена от нескольких поставщиков. Цель облачных вычислений состоит в том, чтобы предоставить услуги по вычислениям и хранению на основе служебных программ или отдельных приложений и возможностей, основанных на бизнес-требованиях, предъявляемых к масштабируемости, доступности и адаптационной способности ожидаемых услуг. В услугах облачных вычислений поставщик обычно называется поставщиком облачных услуг, а приобретающая сторона — заказчиком облачных услуг. В некоторых случаях поставщик облачных услуг делегирует управление или контроль над компонентами, ресурсами и процессами заказчику облачных услуг в среде, потенциально используемой совместно с другими заказчиками облачных услуг, обычно называемой мультитенантной облачной средой. Когда с использованием облачных вычислений формируют цепь поставок ИКТ, например, когда заказчик использует SaaS, который построен поверх IaaS, положения информационной безопасности в цепи поставок ИКТ также применимы.

5.3 Риски в области информационной безопасности в отношениях с поставщиками и связанные с ними угрозы

Риски в области информационной безопасности в отношениях с поставщиками являются поводом для беспокойства не только для покупателя и поставщика, но и для заказчиков и других заинтересованных сторон. Это вопрос доверия к предпринимательской деятельности в обществе. Как поставщик, так и приобретающая сторона должны учитывать изначальные и остаточные риски в области информационной безопасности, связанные с установлением отношений с поставщиком.

Приобретающая сторона и поставщик несут равную ответственность за обеспечение надежности своего соглашения и за управление рисками в области информационной безопасности, которое включает в себя установление определенных ролей и ответственности за информационную безопасность и осуществление мер защиты информации.

Каждое отношение поставщика внутри организации устанавливаются с определенной целью. Число таких отношений, вероятно, будет расти с течением времени, что приведет к тому, что эти отношения не будут полностью управляться или контролироваться стороной, приобретающей услуги. В частности, крупные организации, как правило, имеют значительное число отношений с поставщиками, которые были установлены различными внутренними организациями с использованием различных процессов и договоренностей. Многие из этих связей имеют расширенные цепи поставок с несколькими уровнями. Эта множественность может привести к тому, что организации будет все труднее обеспечить надлежащее устранение рисков в области информационной безопасности, создаваемых такими отношениями с поставщиками.

Поставка и поддержка продукции или услуги может зависеть либо от передачи приобретающей стороны, либо от передачи поставщиком информации и/или информационных систем другой стороне. Эта информация должна быть надлежащим образом защищена путем заключения соглашения между приобретающей стороной и поставщиками. В этом соглашении должен быть определен взаимоприемлемый комплекс мер защиты информации и ответственности за его осуществление. Отсутствие такого соглашения может повлиять на информационную безопасность приобретающей стороны или поставщика из-за:

a) различных методов управления информационной безопасностью у приобретающей стороны и поставщика, пренебрежения отдельными видами рисков и соблюдения сложившейся практики или различных культурных традиций или организационных отношений, приводящих к несоответствию требований и мер безопасности приобретающей стороны и поставщика;

b) доверия к услугам и возможностям поставщика, разрабатываемым для обеспечения соответствия собственным требованиям к информационной безопасности приобретающей стороны, приводящего к непредусмотренной зависимости при управлении;

c) конфликтующих между собой или различных средств контроля информационной безопасности приобретающей стороны и поставщика, которые препятствуют или ослабляют информационную безопасность другой стороны.

Отношения с поставщиками могут создавать ряд рисков в области информационной безопасности как для приобретающей стороны, так и для поставщиков. Ниже приведены примеры таких рисков, которые следует учитывать на протяжении всего жизненного цикла отношений с поставщиком — от стадии планирования до стадии завершения:

a) отсутствие или слабая система управления:

1) приобретающая сторона теряет контроль над тем, как хранится, обрабатывается, передается, создается, изменяется и уничтожается информация;

2) поставщики, если запрет на это не оговорен в соглашении, могут передать часть ресурсов и процессов на аутсорсинг другому поставщику, тем самым уменьшая или ограничивая контроль приобретающей стороны и потенциально подвергая ее дополнительным рискам;

b) отсутствие достаточной коммуникации и недопонимание:

1) меры защиты информации, введенные поставщиком, не учитывают риски, выявленные приобретающей стороной, в результате чего последний становится уязвимым к рискам, которые, как предполагается, должны рассматриваться и управляться поставщиком;

2) требования приобретающей стороны к конфиденциальности, целостности и доступности не могут быть должным образом доведены до сведения поставщика и, следовательно, не соблюдаются надлежащим образом;

3) требования, касающиеся доступности/обеспечения непрерывности бизнеса для информации или информационных систем, которые поддерживают своевременную поставку товаров или услуг поставщиком приобретающей стороне, не могут быть определены, что приводит к перебоям в поставках;

4) поставщики не выделяют достаточных ресурсов, включая квалифицированный персонал, для защиты информации приобретающей стороны.

c) географические, социальные и культурные различия:

1) приобретающая сторона непреднамеренно нарушает законодательство или нормативные акты, что наносит ущерб репутации и приводит к финансовым штрафам;

2) ссылка на закон или стандарт в качестве требования в договоре допускает неверное истолкование приобретающей стороной и поставщиком, что приводит к спору;

3) услуга предоставляется в месте или неизвестном, или не разрешенном приобретающей стороной, что приводит к нарушению соблюдения нормативных требований.

Определенные риски в области информационной безопасности для информации и информационных систем приобретающей стороны и/или поставщика могут быть напрямую связаны с недостаточной осведомленностью о контроле, ответственности и подотчетности. Такие риски могут быть применимы к поставкам как продукции, так и услуг. В таблице 1 приведены примеры рисков в области информационной безопасности, связанных с приобретением продуктов. Риски в области информационной безопасности, связанные с услугами, обычно обусловлены доступом поставщиков к информации или информационным системам. В таблице 2 приведены примеры рисков, связанных с доступом поставщика к информации и информационным системам приобретающей стороны.

Таблица 1 — Пример рисков в области информационной безопасности при приобретении продуктов

№	Тип	Описание
1	Функция защиты информации	В случае, если поставляемые продукты имеют уязвимость, то производные продукты, услуги или процессы приобретающей стороны будут также уязвимы
2	Качество	Низкое качество поставляемой продукции может привести к ослаблению информационной безопасности производных продуктов, услуг и процессов приобретающей стороны
3	Права на интеллектуальную собственность	Неидентифицированные права на интеллектуальную собственность могут впоследствии вызвать спор в отношении производных продуктов или услуг приобретающей стороны

Окончание таблицы 1

№	Тип	Описание
4	Подлинность	В случае поставки поддельных или «пиратских» продуктов, ожидания приобретающей стороны относительно функций информационной безопасности, а также качества и идентификации прав интеллектуальной собственности, находятся под угрозой в связи с вероятностью возникновения проблемы информационной безопасности и утраты доверия к деловым отношениям
5	Гарантии, доверие	Без обеспечения надлежащих характеристик информационной безопасности, качества продукции и идентификации прав интеллектуальной собственности и подлинности приобретающая сторона не может быть уверена в надежности продукции поставщика

Таблица 2 — Пример рисков в области информационной безопасности при приобретении услуг

№	Тип	Описание	Примеры использования
1	Физический доступ на объекте	Поставщик имеет физический доступ к средствам обработки информации приобретающей стороны, но не имеет логического доступа	Услуги охраны, доставки, уборки или технического обслуживания оборудования
2	Доступ к информации и информационным системам на объекте	Персонал поставщика находится на месте и имеет логический доступ к информации и информационным системам приобретающей стороны, посредством использования оборудования последней	Аутсорсинговая экспертиза, проводимая на месте и интегрированная в команду приобретающей стороны
3	Удаленный доступ к внутренней информации и информационным системам	Поставщик имеет удаленный доступ к информации и информационным системам приобретающей стороны	Деятельность по удаленной разработке и техническому обслуживанию, удаленное управление информационными системами и оборудованием, логистика, работа колл-центра, автоматизированные системы управления объектами
4	Обработка информации за пределами объекта	Информация, находящаяся под ответственностью приобретающей стороны, обрабатывается поставщиком за пределами объекта, с использованием приложений и систем, находящихся под контролем и управлением поставщика	Консалтинг (маркетинговые исследования, стимулирование сбыта, технические исследования и др.), обработка информации, НИОКР, производство, хранение и архивирование, служба приложений, Бизнес-процесс как Услуга (BPaaS), такие как туристические или финансовые услуги, инфраструктура как услуга (IaaS) или Программное обеспечение как Услуга (SaaS)
5	Удаленные приложения	Приложения, управляемые приобретающей стороной, работают под управлением PaaS или IaaS	Поставщики платформы как услуги (PaaS), если поставщик предоставляет платформу разработки, или поставщики IaaS, если поставщик предоставляет сетевые, вычислительные и услуги хранения
6	Оборудование за пределами объекта	Оборудование, предназначенное для приобретающей стороны, и которая является его собственником, размещается за пределами объекта, на сайте поставщика	Информационные системы или оказываемая как услуга инфраструктура (IaaS) за пределами объекта

Окончание таблицы 2

№	Тип	Описание	Примеры использования
7	Хранение информации за пределами объекта	Приобретающая сторона передает хранение информации поставщику на аутсорсинг для хранения ее за пределами объекта или для архивирования	Использование службы хранения для поддержания резервных копий информации, генерируемой внутренней обработкой информации
8	Депонирование исходного кода	Услуги, связанные с артефактами поставщика, используемыми приобретающей стороной, депонируются доверенной третьей стороной и предоставляются приобретающей стороне при определенных обстоятельствах	Исходный код хранится независимой третьей стороной для поддержания полезности программного обеспечения приобретающей стороной в случае, если поставщик программного обеспечения выходит из бизнеса

5.4 Управление рисками в области информационной безопасности в отношениях с поставщиками

В отношениях с поставщиком доступ приобретающей стороны или поставщика к информации другой организации или ее обработка могут создавать риски в области информационной безопасности как для приобретающей стороны, так и для поставщика. Приобретающая сторона и поставщик оценивают риски, выбирают, внедряют и поддерживают меры защиты информации для их снижения. В контексте отношений с поставщиками эти меры состоят из:

a) тех, которые непосредственно касаются рисков нарушения информационной безопасности, связанных с доступом и обработкой информации каждой организации;

b) тех, которые касаются качества продукции и услуг поставщика, которые влияют на риски нарушения информационной безопасности приобретающей стороны или ее заказчика;

c) тех, которые направлены на обеспечение a) или b) по отношению к другой организации, например, с помощью разработки требований к управлению и отчетности, мониторинга, аудита и сертификации.

Соглашение между приобретающей стороной и поставщиком обязывает обе организации осуществлять и поддерживать эти меры.

Независимо от характера предоставляемых продукции или услуги, прозрачность информационной безопасности должна рассматриваться как важная часть установления отношений с поставщиком для обеспечения управления рисками в области информационной безопасности для информации и информационных систем приобретающей стороны. Для выявления и управления этими рисками в области информационной безопасности приобретающая сторона должна получить гарантию того, что у поставщика внедрены адекватные системы управления и меры защиты информации. В случае, если это не обсуждается, приобретающая сторона должна выбрать продукт или услугу поставщика на основе критериев, которые включают требования к управлению информационной безопасностью и меры защиты информации для предотвращения или снижения рисков до допустимого уровня.

5.5 Рассмотрение цепи поставок ИКТ

Принятие приобретающей стороной продукции, поставки и эксплуатации продукции и услуг поставщика должно основываться на критериях, обеспечивающих уровень информационной безопасности, который приобретающая сторона желает иметь в своей организации. Они могут включать в себя любое из следующих действий:

- управление рисками политической, правовой и информационной безопасностью, связанными с местной средой, которые влияют на информационную безопасность приобретающей стороны, включая непрерывность информации, информационных систем и услуг;
- обеспечение конфиденциальности информации физических и электронных документов и другой информации, относящейся к поставляемым продуктам и услугам;
- обеспечение целостности материалов и элементов для обеспечения надлежащего обращения, т. е. уникальная маркировка и защитные обозначения;

- обеспечение целостности программного обеспечения или другой электронной информации, относящейся к поставляемому продукту или услуге, чтобы гарантировать, что она не скомпрометирована, т. е. имеются криптографические хэш-функции или цифровые водяные знаки;

- управление физической безопасностью объектов, с которых осуществляется поставка продукции и услуг;

- управление информационной безопасностью, относящейся к любому аспекту деятельности поставщиков, взаимодействию поставщиков с поставщиками и взаимодействию поставщиков с другими приобретающими сторонами.

Для надлежащего управления информационной безопасностью в отношениях с поставщиками по всей цепи поставок ИКТ приобретающей стороне следует принять систему, включающую следующий набор стандартизированных общеорганизационных процессов приобретения продукции и услуг:

a) установить требования к информационной безопасности и соблюдению требований для безопасного обмена или совместного использования информации и информационных систем;

b) до момента приобретения оценить и контролировать риски в области информационной безопасности, связанные с цепью поставок;

c) установить процесс переговоров или повторных переговоров по соглашению о цепи поставок ИКТ или соглашениям, включающим требования к информационной безопасности и соблюдению требований, включая условия для осуществления права на аудит и ограничения поставщиков на фазе постконтроля на всех многочисленных уровнях цепи поставок ИКТ;

d) постоянно контролировать и отчитываться о работе поставщиков в рамках цепи поставок ИКТ, соблюдая требования информационной безопасности и соответствия, особенно в результате изменения отношений с поставщиком.

Эта структура должна быть гибкой, чтобы обеспечить возможность заключения целого ряда соглашений о цепи поставок ИКТ, которые могут быть адаптированы с учетом характера приобретаемых продукции или услуги и рисков, которые они, как ожидается, создадут.

6 Общая структура и обзор ИСО/МЭК 27036

6.1 Назначение и структура

ИСО/МЭК 27036 — это стандарт, состоящий из нескольких частей, который содержит требования и рекомендации для приобретающих сторон и поставщиков по обеспечению безопасности информации в отношениях с поставщиками. На рисунке 2 представлена условная архитектура этого составного международного стандарта.

В частях 3 и 4 рассматриваются конкретные аспекты информационной безопасности во взаимоотношениях с поставщиками, включая проблемы, связанные с продукцией и услугами ИКТ (часть 3) и облачными услугами (часть 4).

Рисунок 2 — ИСО/МЭК 27036 Архитектура

6.2 Обзор части 1: Обзор и основные понятия

Часть 1 (настоящий стандарт) содержит обзор и основные понятия информационной безопасности в отношениях с поставщиками. Часть 1 является справочным документом.

6.3 Обзор части 2: Требования

Часть 2 обеспечивает высокоуровневую основу для установления требований и ожиданий в области информационной безопасности в отношениях с поставщиками. Данная структура включает в себя управление, процессы жизненного цикла и соответствующие заявления о требованиях высокого уровня. Часть 2 — это нормативный стандарт, который приобретающие стороны могут использовать в качестве источника требований к соглашению для определения, управления и мониторинга соглашений с поставщиками. Требования настоящего стандарта могут также служить в качестве дополнительных критериев и в целях сертификации по стандарту ИСО/МЭК 27001 или других схем сертификации, которые считаются уместными для приобретающей стороны. Например, приобретающая сторона может потребовать, чтобы поставщик был сертифицирован в соответствии со стандартом ИСО/МЭК 27001, включающим дополнительные требования и применения мер защиты информации в соответствии с ИСО/МЭК 27036 в отношении предлагаемых продуктов или услуг. Приобретающая сторона может либо использовать весь стандарт, либо извлекать его отдельные части для использования в качестве требований.

6.4 Обзор части 3: Рекомендации по обеспечению безопасности цепи поставок информационных и коммуникационных технологий

В отношениях поставщик — приобретающая сторона приобретаемые продукция или услуги ИКТ, не обязательно должны быть произведены или эксплуатироваться исключительно поставщиком. Например, продукт часто содержит детали, изготовленные другими поставщиками и предоставленные поставщику в качестве косвенных отношений с приобретающей стороной. Или, например, служба обработки информации может быть построена на других службах обработки информации в качестве базовой инфраструктуры. Так, у поставщика есть соглашение с другим поставщиком на обслуживание оборудования, хранение резервных копий вовне или даже на весь процесс резервного копирования, отданный на аутсорсинг. Таким образом, цепь поставок ИКТ формируется последовательными отношениями поставщиков с присущими им взаимозависимостями.

В цепи поставок управление обеспечением информационной безопасностью и контроль, осуществляемый поставщиком в непосредственных отношениях с приобретающей стороной, не всегда достаточны для управления рисками в области информационной безопасности продукции или услуги. Управление приобретающей стороной продуктом или услугой косвенного поставщика (который является поставщиком поставщика) может иметь важное значение для обеспечения информационной безопасности: для этого необходима прозрачность в цепи поставок.

И наоборот, поставщики могут также испытывать повышенные риски в области информационной безопасности, вызванные взаимосвязанностью систем приобретающей стороны и поставщика, которая иногда является результатом цепи поставок ИКТ. Например, покупатель может потребовать полного (инвазивного) аудита систем поставщика, что может привести к доступу покупателя к интеллектуальной собственности поставщика.

Часть 3 ИСО/МЭК 27036 содержит руководящие принципы для приобретающих сторон и поставщиков по управлению рисками в области информационной безопасности, связанными с цепью поставок продукции и услуг ИКТ. Он основывается на требованиях, изложенных в части 2, и содержит дополнительные методы, дополняющие требования высокого уровня, содержащиеся в части 2.

6.5 Обзор части 4: Рекомендации по обеспечению безопасности облачных услуг

Организации используют услуги облачных вычислений, чтобы воспользоваться преимуществами положительного эффекта от масштаба, обеспечиваемого гибкими возможностями по оказанию услуг обработки и хранения. Эти возможности доступны благодаря модели использования или модели на основе полезности. Облачные вычисления могут предоставляться в различных моделях предоставления облачных услуг, например в IaaS, PaaS и SaaS. Однако это ведет к возникновению рисков в области информационной безопасности, связанных с более сложной взаимосвязанностью систем приобретающей стороны и поставщика. Как и в случае с рисками в области информационной безопасности в цепи поставок ИКТ, существует возможность отсутствия ясности в отношении ролей и обязанностей по управлению информационной безопасностью и осуществлению контроля.

Например, если информация при рабочих нагрузках облачных вычислений пересекает национальные границы или клиент облачной услуги не может контролировать предоставление облачной услуги, это может привести к рискам нарушения требований, законодательных или иных нормативных

правовых актов со стороны любой приобретающей стороны или поставщика. Кроме того, мульти-аренда и использование технологий (например, виртуализация и прикладные программные интерфейсы), может привести к новым рискам в области информационной безопасности и обеспечения конфиденциальности облачных заказчиков в результате неадекватного контроля доступа и отсутствия разделения заказчиков облачных услуг.

Часть 4 ИСО/МЭК 27036 содержит руководящие принципы информационной безопасности облачных вычислительных услуг, которые часто предоставляются по цепи поставок с точки зрения как приобретающей стороны, так и поставщика таких услуг. В частности, она включает в себя управление рисками в области информационной безопасности, связанными с облачными вычислительными услугами на протяжении всего жизненного цикла отношений с поставщиками. Она основывается на требованиях, изложенных в части 2, и содержит дополнительные методы, которые могут дополнить требования высокого уровня, содержащиеся в части 2, и рекомендации, содержащиеся в части 3.

Приложение ДА
(справочное)

Сведения о соответствии ссылочного международного стандарта национальному стандарту

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 27000	IDT	ГОСТ Р ИСО/МЭК 27000—2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта:

- IDT — идентичный стандарт.

Библиография

[1] ISO/IEC 15288, Systems and software engineering — System life cycle processes

[2] ISO/IEC 12207, Systems and software engineering — Software life cycle processes

[3] ISO/IEC 20000, Information technology — Service management — Part 1: Service management system requirements

[4] ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

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

[6] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls

[7] ISO/IEC 27005, Information technology — Security techniques — Information security risk management

[8] ISO/IEC 27014, Information technology — Security techniques — Governance of information security

[9] ISO/IEC 27035, Information technology — Security techniques — Information security incident management

[10] ISO 28000, Specification for security management systems for the supply chain

[11] ISO 28001, Security management systems for the supply chain — Best practices for implementing supply chain security assessments and plans — Requirements and guidance

[12] ISO 9000:2005, Quality management systems — Fundamentals and vocabulary

УДК 006.34:004.056:004.056.5:004.056.53:006.354 ОКС 35.040

Ключевые слова: информационная безопасность, информационные технологии, методы и средства обеспечения безопасности, поставщик, приобретающая сторона, риск, информационные системы

Редактор *Д.А. Кожемяк*
Технический редактор *И.Е. Черепкова*
Корректор *Р.А. Ментова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 24.05.2021. Подписано в печать 03.06.2021. Формат 60×84¼. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,10.

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