ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р 59215— 2020

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВО ВЗАИМООТНОШЕНИЯХ С ПОСТАВЩИКАМИ

Часть 3

Рекомендации по обеспечению безопасности цепи поставок информационных и коммуникационных технологий

(ISO/IEC 27036-3:2013, NEQ)

Издание официальное

Москва
Стандартинформ
2020

gost.e-ecolog.ru

Предисловие

1 РАЗРАБОТАН Федеральным государственным учреждением «Федеральный исследовательский центр «Информатика и управление» Российской академии наук» (ФИЦ ИУ РАН) и Акционерным обществом «Научно-производственное объединение «Эшелон» (АО «НПО «Эшелон»)

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 26 ноября 2020 г. № 1191-ст

4 Настоящий стандарт разработан с учетом основных нормативных положений международного стандарта ИСО/МЭК 27036-3:2013 «Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 3. Рекомендации по обеспечению безопасности цепи поставок информационных и коммуникационных технологий» (ISO/IEC 27036-3:2013 «Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security», NEQ)

5 ВВЕДЕН ВПЕРВЫЕ

*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 (*gost.e-ecolog.ru

© ISO/IEC, 2018 — Все права сохраняются
© Стандартинформ, оформление, 2020

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины, определения и сокращения 2
4 Основные понятия 2
4.1 Сценарий для обеспечения безопасности цепи поставок информационных и коммуникационных технологий 2
4.2 Риски в цепи поставок информационных и коммуникационных технологий и связанные с ними угрозы 2
4.3 Типы взаимоотношений между приобретающей стороной и поставщиком 3
4.4 Организационные возможности 3
4.5 Процессы жизненного цикла системы 4
4.6 Процессы системы менеджмента информационной безопасности по отношению к процессам жизненного цикла системы 4
4.7 Меры системы менеджмента информационной безопасности в отношении обеспечения безопасности цепи поставок информационных и коммуникационных технологий 5
4.8 Основные методы обеспечения безопасности цепи поставок информационных и коммуникационных технологий 5
5 Безопасность цепи поставок информационных и коммуникационных технологий в процессах жизненного цикла 6
5.1 Процессы соглашения 6
5.2 Процессы организационного обеспечения проекта 9
5.3 Процессы технического управления 11
5.4 Технические процессы 13
Приложение А (справочное) Сопоставление мер раздела 5 настоящего стандарта с мерами, рекомендуемыми другими стандартами в области информационной безопасности . . . 20

Введение

ИСО (Международная организация по стандартизации) и МЭК (Международная электротехническая комиссия) образуют специализированную систему Всемирной стандартизации. Национальные органы, которые являются членами ИСО или МЭК, участвуют в развитии международных стандартов посредством технических комитетов, учрежденных соответствующей организацией для рассмотрения конкретных областей технической деятельности. Технические комитеты ИСО и МЭК сотрудничают в областях, представляющих взаимный интерес. Правительственные и неправительственные организации в сотрудничестве с ИСО и МЭК также принимают участие в работе. В области информационных технологий ИСО и МЭК учредили совместный технический комитет ИСО/МЭК СТК 1. Международные стандарты разрабатываются в соответствии с правилами, приведенными в части 2 директив ИСО/МЭК (см. gost.e-ecolog.ru).

Основные положения и меры обеспечения информационной безопасности установлены в ГОСТ Р ИСО/МЭК 27001 и ГОСТ Р ИСО/МЭК 27002. Дополнительную информацию о конкретных требованиях при установлении и контроле взаимоотношений с поставщиками содержит серия стандартов ИСО/МЭК 27036 «Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками», подготовленная совместным техническим комитетом ИСО/МЭК СТК 1 «Информационные технологии (ИТ)», подкомитетом SC 27 «Методы и средства обеспечения информационной безопасности ИТ» и включающая:

- 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.

В настоящем стандарте наименования процессов жизненного цикла систем и их описания соответствуют ГОСТ Р 57193. Настоящий стандарт содержит ссылки на соответствующие меры обеспечения информационной безопасности, установленные в ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27004 и ГОСТ Р ИСО/МЭК 27005.

Продукция и услуги в области информационных и коммуникационных технологий (ИКТ) разрабатываются, комплексируются и поставляются на глобальном уровне через длинные и физически разрозненные цепи поставок. Продукция ИКТ собирается из многих компонентов, предоставляемых многими поставщиками. Услуги ИКТ в рамках всех взаимоотношений с поставщиками также предоставляются на основе нескольких уровней аутсорсинга и цепи поставок. Потребители не имеют информации о поставщиках оборудования, программного обеспечения и услуг далее одной (максимум двух) ступеней в цепи поставки. С существенным увеличением числа организаций и физических лиц, имеющих отношение к продукции или услуге ИКТ, прозрачность процесса объединения этих продуктов и услуг существенно снижается. Отсутствие наглядности, прозрачности и прослеживаемости в цепи поставок ИКТ создает риски для организаций-потребителей.

Настоящий стандарт содержит рекомендации для приобретающих сторон и поставщиков продукции и услуг ИКТ по снижению или управлению рисками в области информационной безопасности. В настоящем стандарте определяются бизнес-обоснование безопасности цепи поставок ИКТ, конкретные риски и типы отношений, а также способы развития организационных возможностей для управления аспектами информационной безопасности и включения подхода, связанного с жизненным циклом, для управления рисками с поддержкой конкретными мерами, средствами и практикой. Ожидается, что его применение приведет к:

- повышению наглядности, прозрачности и прослеживаемости цепи поставок ИКТ для повышения возможностей информационной безопасности;
- более глубокому пониманию приобретающей стороной того, откуда берется их продукция или услуги, и методов, используемых для разработки, комплексирования или применения этой продукции или услуг, для повышения эффективности выполнения требований информационной безопасности;
- в случае компрометации информационной безопасности — наличию информации о том, что могло быть скомпрометировано и кем могут быть вовлеченные в это субъекты.

Настоящий стандарт предназначен для использования всеми типами организаций, которые приобретают или поставляют продукцию и услуги в цепи поставок ИКТ. Руководство в первую очередь ориентировано на первоначальную связь первого звена «приобретающая сторона — поставщик», но основные шаги должны применяться по всей цепи, начиная с того момента, когда первоначальный

поставщик меняет свою роль на роль приобретающей стороны и т. д. Это изменение ролей и применение одних и тех же шагов для каждого нового звена «приобретающая сторона — поставщик» в цепочке является основной причиной разработки настоящего стандарта. В соответствии с настоящим стандартом последствия для информационной безопасности могут передаваться между организациями по цепочке. Это помогает выявить риски в области информационной безопасности и их причины и может повысить прозрачность всей цепи поставок. Проблемы информационной безопасности, связанные с взаимоотношениями с поставщиками, охватывают широкий спектр сценариев. Организации, желающие повысить уровень доверия в рамках своей цепи поставок ИКТ, должны определить свои границы доверия, оценить риск, связанный с их действиями в рамках цепи поставок, а затем определить и реализовать соответствующие методы выявления и снижения риска возникновения уязвимостей в рамках своей цепи поставок ИКТ.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ВО ВЗАИМООТНОШЕНИЯХ С ПОСТАВЩИКАМИ

Часть 3

Рекомендации по обеспечению безопасности цепи поставок информационных и коммуникационных технологий

Information technology. Security techniques. Information security for supplier relationships. Part 3. Guidelines for information and communication technology supply chain security

Дата введения — 2021—06—01

1 Область применения

Настоящий стандарт содержит рекомендации по обеспечению безопасности цепи поставок информационных и коммуникационных технологий (ИКТ) для приобретающей стороны и поставщиков:

а) по получению информации о рисках в области информационной безопасности, вызванных физически рассредоточенными и многоуровневыми цепями поставок ИКТ, и управлению ими;

б) по реагированию на риски, связанные с глобальной цепью поставок продукции и услуг ИКТ, которые могут оказать влияние на информационную безопасность организаций, использующих эти продукцию и услуги. Эти риски могут быть связаны как с организационными, так и с техническими аспектами (например, с внедрением вредоносного кода или с наличием контрафактной продукции на рынке ИКТ);

в) по интеграции процессов и методов обеспечения информационной безопасности (см. ГОСТ Р ИСО/МЭК 27002) в процессы жизненного цикла системы и программного обеспечения (см. ГОСТ Р 57193 и ГОСТ Р ИСО/МЭК 12207).

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие стандарты:

ГОСТ Р ИСО/МЭК 12207 Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств

ГОСТ Р ИСО/МЭК 27000 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология

ГОСТ Р ИСО/МЭК 27001 Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования

ГОСТ Р ИСО/МЭК 27002 Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

ГОСТ Р ИСО/МЭК 27004 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Измерения

ГОСТ Р ИСО/МЭК 27005 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности

Издание официальное

ГОСТ Р ИСО/МЭК 27036-2 Информационные технологии. Методы и средства обеспечения безопасности. Информационная безопасность во взаимоотношениях с поставщиками. Часть 2. Требования

ГОСТ Р 57193 Системная и программная инженерия. Процессы жизненного цикла систем

Примечание — При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов в информационной системе общего пользования — на официальном сайте Федерального агентства по техническому регулированию и метрологии в сети Интернет или по ежегодному информационному указателю «Национальные стандарты», который опубликован по состоянию на 1 января текущего года, и по выпускам ежемесячного информационного указателя «Национальные стандарты» за текущий год. Если заменен ссылочный стандарт, на который дана недатированная ссылка, то рекомендуется использовать действующую версию этого стандарта с учетом всех внесенных в данную версию изменений. Если заменен ссылочный стандарт, на который дана датированная ссылка, то рекомендуется использовать версию этого стандарта с указанным выше годом утверждения (принятия). Если после утверждения настоящего стандарта в ссылочный стандарт, на который дана датированная ссылка, внесено изменение, затрагивающее положение, на которое дана ссылка, то это положение рекомендуется применять без учета данного изменения. Если ссылочный стандарт отменен без замены, то положение, в котором дана ссылка на него, рекомендуется применять в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 В настоящем стандарте применены термины по ГОСТ Р ИСО/МЭК 12207, ГОСТ Р ИСО/МЭК 27000, ГОСТ Р ИСО/МЭК 27036-2 и ГОСТ Р 57193, а также следующие термины с соответствующими определениями:

3.1.1 **прозрачность:** Свойство системы или процесса обеспечивать открытость и подотчетность.

3.1.2 **прослеживаемость:** Свойство, позволяющее отслеживать активность идентификатора, процесса или элемента по всей цепи поставок.

3.2 В настоящем стандарте использованы следующие сокращения:

ИКТ — информационные и коммуникационные технологии;

СМИБ — система менеджмента информационной безопасности.

4 Основные понятия

4.1 Сценарий для обеспечения безопасности цепи поставок информационных и коммуникационных технологий

Организации приобретают продукцию и услуги ИКТ у многочисленных поставщиков, которые, в свою очередь, могут приобретать компоненты у других поставщиков. Снижение рисков в области информационной безопасности, связанных с разрозненными и многоуровневыми цепями поставок ИКТ, может быть достигнуто с использованием методов управления рисками и доверительных отношений, повышая тем самым наглядность, прозрачность и прослеживаемость в цепи поставок ИКТ. Например, повышение наглядности в цепи поставок ИКТ достигается путем определения адекватных требований к информационной безопасности и качеству, а также постоянного мониторинга поставщиков и их продукции и услуг в рамках существующих взаимоотношений с поставщиками. Выявление и отслеживание отдельных лиц, ответственных за качество и безопасность критических элементов, обеспечивает высокую прослеживаемость. Установление договорных требований и ожиданий, а также обзор процессов и практики обеспечивают необходимую прозрачность.

Приобретающая сторона должна донести до сотрудников в своих организациях понимание рисков, связанных с цепью поставок ИКТ, и их возможного воздействия на предприятия. В частности, руководство приобретающей стороны должно знать, что практика поставщиков по всей цепи поставок может повлиять на доверие к продукции и услугам с позиций безопасности бизнеса, информации и информационных систем.

4.2 Риски в цепи поставок информационных и коммуникационных технологий и связанные с ними угрозы

В цепи поставок усилий отдельной организации (приобретающей стороны или поставщика) по управлению информационной безопасностью недостаточно для поддержания информационной безопасности продукции или услуг ИКТ на протяжении всей цепи поставок. Управление приобретающей стороны поставщиками, продукцией или услугами в области ИКТ имеет важное значение для обеспечения информационной безопасности.

Приобретение продукции и услуг ИКТ связано с особыми рисками для приобретающей стороны с точки зрения управления информационной безопасностью. По мере того как глобальные цепи поставок ИКТ становятся физически все более разрозненными и пересекают многочисленные международные и организационные границы, становится все труднее отслеживать конкретные производственные и операционные практики, применяемые к отдельным элементам ИКТ (продуктам, услугам и их компонентам), включая выявление лиц, ответственных за качество и безопасность этих элементов. Это затрудняет прослеживаемость по всей цепи поставок ИКТ, что может привести к более высокому риску:

- компрометации информационной безопасности приобретающей стороны и, следовательно, деловых операций посредством преднамеренных событий, таких как вставка вредоносного кода и наличие контрафактной продукции в цепи поставок ИКТ;
- непреднамеренных событий, таких как использование неадекватных методов разработки программного обеспечения.

Как преднамеренные, так и непреднамеренные события могут привести к компрометации данных и операций приобретающей стороны, включая кражу интеллектуальной собственности, утечку данных и снижение способности приобретающей стороны выполнять свои функции. Любая из этих выявленных проблем, если она возникает, может нанести ущерб репутации организации, что приведет к дальнейшим последствиям, таким как потеря бизнеса.

4.3 Типы взаимоотношений между приобретающей стороной и поставщиком

Приобретающие стороны и поставщики продукции и услуг ИКТ могут вовлекать несколько субъектов в различные отношения, основанные на цепи поставок, включая, но не ограничиваясь следующим:

а) поддержку управления системами ИКТ, когда системы принадлежат приобретающей стороне и управляются поставщиком;

б) системы ИКТ или поставщиков услуг, где системы или ресурсы принадлежат поставщику и управляются им;

в) разработку, проектирование, инженерию и сборку продукции, когда поставщик предоставляет все или часть услуг, связанных с созданием продукции ИКТ;

г) поставку готовых коммерческих продуктов;

д) поставку и распределение продукции с открытым исходным кодом.

Уровень риска приобретающей стороны и потребность в доверии во взаимоотношениях с поставщиками повышаются при предоставлении поставщику более широкого доступа к информации и информационным системам приобретающей стороны и ее зависимости от поставляемых продукции и услуг ИКТ. Например, приобретение поддержки управления системами ИКТ иногда сопряжено с более высоким риском, чем приобретение готовой продукции с открытым исходным кодом или коммерческих продуктов. С точки зрения поставщика любые компрометации в отношении информации приобретающей стороны могут нанести ущерб репутации и доверию поставщика к конкретной приобретающей стороне, информация и информационные системы которой были скомпрометированы.

Чтобы помочь справиться с неопределенностью и рисками, связанными с взаимоотношениями, приобретающие стороны и поставщики должны наладить диалог и достичь понимания в части взаимных ожиданий относительно защиты информации и информационных систем друг друга.

4.4 Организационные возможности

Для управления рисками, связанными с цепью поставок ИКТ на протяжении всего жизненного цикла продукции и услуг, приобретающая сторона и поставщики должны реализовать свои организационные возможности. Эти возможности следует использовать для установления задач в обеспечении безопасности в цепи поставок ИКТ для приобретающей стороны и контролировать выполнение этих задач, включая, как минимум:

а) определение, выбор и реализацию стратегии управления рисками в области информационной безопасности, вызванными уязвимостями в цепи поставок ИКТ, в частности:

1) разработку и поддержание плана превентивного выявления потенциальных уязвимостей, связанных с цепями поставок ИКТ;

2) разработку и поддержание плана нейтрализации негативных последствий;

3) выявление и регистрацию рисков в области информационной безопасности, обусловленных угрозами, уязвимостями и последствиями и связанных с цепью поставок ИКТ (см. 5.3.4);

б) определение/формирование и соблюдение основных мер по обеспечению информационной безопасности в качестве предварительного условия для установления надежных взаимоотношений с поставщиками (см. приложение А);

в) определение/формирование основных процессов и практик в жизненном цикле систем и программного обеспечения для установления надежных взаимоотношений с поставщиками относительно проблем управления рисками в области информационной безопасности цепи поставок ИКТ (см. раздел 5);

г) определение набора базовых требований к информационной безопасности, применимых ко всем взаимоотношениям с поставщиками, и при необходимости адаптацию их для конкретных поставщиков;

д) определение повторяющихся и проверяемых процессов для установления требований информационной безопасности, связанных с новыми взаимоотношениями с поставщиками, управления существующими взаимоотношениями, верификации и подтверждения того, что поставщики соблюдают требования приобретающей стороны, и для прекращения взаимоотношений с поставщиками;

е) определение методов управления изменениями, обеспечивающих своевременное утверждение и применение изменений, потенциально влияющих на информационную безопасность;

ж) определение методов выявления и управления инцидентами, связанными с цепью поставок ИКТ или вызванными ею, а также обмена информацией об инцидентах.

4.5 Процессы жизненного цикла системы

Процессы жизненного цикла системы могут помочь установить взаимоотношения между приобретающей стороной и поставщиками, касающиеся требований и подотчетности по информационной безопасности. Приобретающая сторона может реализовать процессы жизненного цикла внутри компании, чтобы повысить результативность в установлении и управлении взаимоотношениями с поставщиками. Поставщики могут реализовать процессы жизненного цикла для демонстрации результативности в отношении процессов системы и программного обеспечения. В начале работы по реагированию на риски в эти процессы следует включить дополнительные действия по обеспечению информационной безопасности цепей поставок ИКТ.

Использование ГОСТ Р 57193 и ГОСТ Р ИСО/МЭК 12207 позволяет сформировать определенный подход к управлению рисками, связанными с цепью поставок ИКТ. Подход основан на использовании набора одних и тех же процессов, применимых к конкретному контексту систем и программного обеспечения в рамках жизненного цикла или любого этапа жизненного цикла в зависимости от обстоятельств. Например, процесс управления конфигурацией может использоваться как во время разработки, так и в процессе функционирования и сопровождения системы или программного обеспечения. Настоящий стандарт использует тот же подход, описывая каждый процесс в общем виде с использованием формулировки цели, достигаемой решением отдельных задач.

В 4.6 приведено краткое изложение конкретных методов обеспечения безопасности цепи поставок ИКТ. В разделе 5 приведены действия по обеспечению безопасности цепи поставок ИКТ для каждого процесса жизненного цикла. Приобретающая сторона и поставщики должны выбирать те действия, которые имеют отношение к возможностям их организации в области взаимоотношений, а также к индивидуальным отношениям исходя из уровня рисков поставщиков и приобретающей стороны, описанных в 4.1.

4.6 Процессы системы менеджмента информационной безопасности по отношению к процессам жизненного цикла системы

Реализация риск-ориентированной системы менеджмента информационной безопасности (СМИБ) в рамках определенной области — по ГОСТ Р ИСО/МЭК 27001. Наличие СМИБ как в организациях, представляющих приобретающую сторону, так и в организациях-поставщиках поможет приобретающим сторонам и поставщикам приступить к реагированию на риски в цепи поставок ИКТ и осознать необходимость конкретных мер, средств и процессов обеспечения информационной безопасности, необходимых для реагирования на риски.

Примечание — Применение СМИБ предполагает наличие определенной части организации, которая устанавливает и поддерживает взаимоотношения приобретающей стороны и поставщика.

Если организация определяет риски, присущие цепи поставок ИКТ, то должны быть выбраны конкретные меры и средства, которые снижают эти риски с добавлением мер для более полного учета

рисков. В 4.5 использование мер и средств обеспечения информационной безопасности распределено по процессам. В приложении А конкретные меры обеспечения информационной безопасности сопоставлены с отдельными процессами жизненного цикла из раздела 5.

Поставщики могут продемонстрировать приобретающей стороне то, что они имеют определенный уровень зрелости, демонстрируя соответствие ГОСТ Р ИСО/МЭК 27001.

Когда приобретающая сторона и поставщики устанавливают СМИБ, полученную информацию следует использовать для передачи статуса управления информационной безопасностью между приобретающей стороной и поставщиком. Это может охватывать.

а) сферу применения СМИБ;
б) утверждение о применимости;
в) процедуры оценки рисков,
г) план аудита;
д) программы повышения осведомленности;
е) управление инцидентами;
ж) программы измерений;
и) схему классификации информации;
к) управление изменениями;
л) применение других соответствующих специальных мер обеспечения безопасности.

4.7 Меры системы менеджмента информационной безопасности в отношении обеспечения безопасности цепи поставок информационных и коммуникационных технологий

Множество мер обеспечения информационной безопасности и конкретные рекомендации по взаимоотношениям с поставщиками описаны в ГОСТ Р ИСО/МЭК 27002. Эти и дополнительные меры и рекомендации могут использоваться в контексте процессов жизненного цикла систем для оказания помощи приобретающей стороне в проведении валидации конкретных мер и методов поставщика (см. приложение А).

4.8 Основные методы обеспечения безопасности цепи поставок информационных и коммуникационных технологий

Некоторые риски в цепи поставок ИКТ могут быть выявлены на основе применения стандартов, определяющих процессы жизненного цикла систем (см. ГОСТ Р 57193 и ГОСТ Р ИСО/МЭК 12207) и устанавливающих требования к созданию СМИБ (см ГОСТ Р ИСО/МЭК 27001) и мерам обеспечения информационной безопасности (см. ГОСТ Р ИСО/МЭК 27002). Для адекватной реакции на эти риски требуются более подробные практические методы, такие как:

а) цепочка прослеживаемости: приобретающая сторона и поставщик должны быть уверены в том, что каждое изменение и передача, проведенные в течение срока службы элемента, санкционированы, прозрачны и поддаются верификации;

б) доступ с наименьшими привилегиями: персонал может получить доступ к важной информации и информационным системам только с привилегиями, которые необходимы для выполнения своей работы;

в) разделение обязанностей: управление процессом создания, изменения или удаления данных или процессом разработки, эксплуатации или удаления аппаратного и программного обеспечений исходя из того, что ни один человек или функция не имеют возможность самостоятельно выполнить задачу;

г) сопротивление несанкционированному вмешательству и наличие доказательства: попытки подделки должны быть затруднены, а когда они случаются — выявляемыми с возможностью исправления;

д) постоянная защита: критические данные должны быть защищены способами, которые остаются эффективными, даже если эти данные передаются из места их создания или изменения;

е) управление соответствием: приемлемость мер защиты в рамках соглашения может постоянно и независимо подтверждаться;

ж) оценка и верификация кода: применяются методы верификации кода, подозрительный код выявляется;

и) подготовка кадров по вопросам безопасности цепи поставок ИКТ: способность организации эффективно обучать соответствующий персонал методам обеспечения информационной безопасности.

Обучение должно включать в себя изучение безопасных методов разработки, методов распознавания фальсификации и иное по мере необходимости:

к) оценка уязвимости и ответные меры: формальное понимание приобретающей стороной того, насколько хорошо их поставщики оснащены возможностями для сбора информации об уязвимостях от исследователей, клиентов или источников, а также для проведения содержательного анализа воздействия на уязвимости и принятия надлежащих мер реагирования в короткие сроки. Это должно включать в себя соглашение между приобретающей стороной и поставщиком о систематических повторяющихся процессах реагирования на уязвимость;

л) определенные ожидания: в соглашении излагаются четкие формулировки требований, предъявляемых к элементу и среде проектирования/разработки. Эти требования должны включать в себя обязательство обеспечить тестирование по требованиям информационной безопасности, исправления кода и гарантии в отношении используемых процессов разработки, интеграции и доставки;

м) права собственности и обязанности: в соглашении должны быть определены права собственности приобретающей стороны и поставщика на интеллектуальную собственность и обязанности другой стороны по защите прав интеллектуальной собственности;

н) избегание компонентов «серого рынка»: многих рисков в цепи поставок ИКТ можно избежать, требуя верификации подлинности компонентов системы;

п) анонимное приобретение: когда это уместно и возможно, следует практиковать анонимное приобретение (т. е. когда личность приобретающей стороны заинтересована в анонимности), затенять связь между цепью поставок ИКТ и приобретающей стороной;

р) единовременное приобретение: компоненты для систем с длительным сроком службы (надежные автоматические средства обеспечения безопасности) могут устареть и тем самым увеличить риски в цепи поставок ИКТ. Приобретение нужных запасных частей в течение определенного периода времени снижает эти риски;

с) рекурсивные требования к поставщикам: контракты могут определять, что поставщики устанавливают и подтверждают требования к цепи поставок ИКТ для вышестоящих поставщиков.

5 Безопасность цепи поставок информационных и коммуникационных технологий в процессах жизненного цикла

5.1 Процессы соглашения

Взаимоотношения между приобретающими сторонами и поставщиками достигаются с использованием соглашений. Организации могут выступать одновременно или последовательно в качестве как приобретающих сторон, так и поставщиков продукции и услуг ИКТ. В тех случаях, когда приобретающая сторона и поставщик находятся внутри одной организации, рекомендуется по-прежнему использовать процессы соглашения, но с меньшей формальностью. Процессы соглашения включают в себя процесс приобретения и процесс поставки.

Дополнительные специальные рекомендации относительно процессов соглашения см. в ГОСТ Р ИСО/МЭК 27002. Сопоставление положений настоящего подраздела с мерами обеспечения информационной безопасности, рекомендуемыми ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27004, ГОСТ Р ИСО/МЭК 27005, приведено в приложении А.

5.1.1 Процесс приобретения

Целью процесса приобретения является получение продукции или услуги в соответствии с требованиями приобретающей стороны. Рекомендации по внедрению процесса приобретения см. в ГОСТ Р 57193. Приобретающей стороне для обеспечения надлежащего управления рисками в цепи поставок ИКТ следует выполнять следующие действия:

а) готовиться к приобретению:

1) определять стратегию того, как будет осуществляться приобретение:

- устанавливать стратегии поиска источников, основанные на понятии допустимости рисков в области информационной безопасности в отношении цепи поставок ИКТ;
- задавать набор базовых требований к информационной безопасности, применимых ко всем взаимоотношениям с поставщиками;

2) адаптировать набор базовых требований к информационной безопасности для конкретных взаимоотношений с поставщиками, чтобы подготовить запрос на поставку продукции или услуги:

- устанавливать требования к информационной безопасности для поставщиков, включая связанные с ИКТ нормативные требования (например, к телекоммуникациям или информационным технологиям), технические требования, цепь хранения, наглядность и прозрачность, обмен информацией об инцидентах информационной безопасности по всей цепи поставок, правила удаления или хранения таких компонентов, как данные или интеллектуальная собственность, другие соответствующие требования;

- устанавливать требования к поставщикам, управляющим своими поставщиками в цепи поставок ИКТ, если это необходимо;

- определять требования к поставщикам в цепи поставок ИКТ для предоставления достоверных доказательств того, что они выполнили требования информационной безопасности;

- определять требования к поставщикам критических элементов в цепи поставок ИКТ для демонстрации способности устранять возникающие уязвимости на основе информации, полученной от приобретающих сторон других источников, а также реагировать на инциденты и устранять те уязвимости, которые привели к инциденту;

- определять требования к владению интеллектуальной собственностью и ответственность приобретающей стороны и поставщиков в отношении таких элементов, как программный код, данные и информация, среда производства/разработки/интеграции, проекты и процессы, находящиеся в собственности;

- определять требования к поставщикам в части ожидаемого срока службы элемента, чтобы помочь приобретающей стороне планировать любую поставку, которая может потребоваться для поддержки функционирования системы;

- определять требования к аудиту информационных систем поставщиков, где это приемлемо;

- определять требования для мониторинга рабочих процессов поставщиков и рабочих продуктов, где это приемлемо;

- определять требования для передачи их от вышестоящих поставщиков нижестоящим, чтобы распределить требования приобретающей стороны по всей цепи поставок;

б) рекламировать приобретение и выбирать поставщика:

1) сообщать запрос на поставку продукции или услуги определенным поставщикам — здесь не требуется никаких специальных действий, связанных с цепью поставок ИКТ;

2) выбирать одного или нескольких поставщиков:

- отбирать поставщиков на основе оценки их способности удовлетворять определенным требованиям, в том числе предъявляемым к цепи поставок ИКТ;

- использовать установленные методы оценки и результаты оценок для продукции, услуг, компонентов ИКТ или их поставщиков в качестве критериев оценки соответствия установленным требованиям (например, для сертификации СМИБ у поставщиков);

- учитывать в рамках исходных требований и процессов опыт предыдущей деятельности поставщиков в отношении кадровой политики, процедур и практических методов обеспечения информационной безопасности;

в) заключать и сопровождать соглашение:

1) проводить переговоры с выбранным поставщиком или поставщиками, предусматривая включение в соглашение согласованных требований, применимых к цепи поставок ИКТ;

2) заключать соглашение с поставщиком, в рамках которого разработать и сопровождать план обеспечения целостности приобретенных программных и аппаратных продуктов и компонентов, предоставляемых по цепи поставок ИКТ;

г) контролировать соглашение:

1) оценивать исполнение соглашения:

- устанавливать и поддерживать процедуры и критерии верификации для поставляемых продукции и услуг;

- проводить аудит информационных систем поставщиков, где это приемлемо;

- осуществлять контроль и оценку процессов поставщиков (например, проекта, практики поставок и т. д.) и рабочих продуктов, где это приемлемо;

2) своевременно предоставлять необходимые данные поставщику и разрешать возникающие вопросы, в частности сообщать о недостатках в обеспечении информационной безопасности и

уязвимостях, обнаруженных при использовании продукции или услуг, предоставляемых по цепи поставок ИКТ;

3) оценивать поставщиков на предмет их способности удовлетворять определенным требованиям в цепи поставок ИКТ;

д) принимать продукт или услугу:

1) подтверждать, что поставленный продукт или услуга соответствуют соглашению, — здесь не требуется никаких специальных действий, связанных с цепью поставок ИКТ;

2) проводить оплату или предоставлять поставщику другое согласованное действие за товар или услугу, необходимое для закрытия соглашения, — здесь не требуется никаких специальных действий, связанных с цепью поставок ИКТ.

5.1.2 Процесс поставки

Цель процесса поставки заключается в обеспечении приобретающей стороны продукцией или услугами, удовлетворяющими согласованным требованиям. Поставщику для обеспечения надлежащего управления рисками в цепи поставок ИКТ следует выполнять следующие действия:

а) готовиться к поставке: определять факт наличия представителя приобретающей стороны, у которого есть организация или который представляет организацию или организации, нуждающиеся в продукции или услуге, — здесь не требуется никаких специальных действий, связанных с цепью поставок ИКТ;

б) отвечать на запрос (тендер):

1) оценивать запрос о поставке продукции или услуги, чтобы определить выполнимость и содержание ответа, — следует указывать набор базовых требований к информационной безопасности, которые применяются ко всем взаимоотношениям с приобретающей стороной, с адаптацией по мере необходимости;

2) готовить ответ, который удовлетворяет запросу:

- устанавливать способ демонстрации возможности поставлять продукцию и услуги, которые отвечают требованиям информационной безопасности приобретающей стороны, включая связанные с ИКТ нормативные требования, технические требования, цепочку хранения, наглядность и прозрачность, обмен информацией об инцидентах информационной безопасности по всей цепи поставок, правила удаления компонентов или хранения таких компонентов, как данные или интеллектуальная собственность, и другие соответствующие требования;

- адаптировать набор базовых требований к информационной безопасности для конкретных взаимоотношений с приобретающей стороной по мере необходимости;

- указывать требования к предоставлению достоверных доказательств о соблюдении требований, предъявляемых приобретающей стороной;

в) заключать и поддерживать соглашение:

1) заключать соглашение с приобретающей стороной — здесь не требуется никаких специальных действий, связанных с цепью поставок ИКТ;

2) начинать реализовывать соглашение с приобретающей стороной:

- разрабатывать и сопровождать план обеспечения целостности включенных и поставляемых программных и аппаратных продуктов и компонентов;

- разрабатывать и сопровождать план обеспечения защиты прав на интеллектуальную собственность;

г) выполнять соглашение:

1) выполнять соглашение в соответствии с утвержденными поставщиком проектными планами — здесь не требуется никаких специальных действий, связанных с цепью поставок ИКТ;

2) оценивать выполнение соглашения — здесь не требуется никаких специальных действий, связанных с цепью поставок ИКТ;

д) поставлять и сопровождать продукт или услугу:

1) поставлять продукт или услугу в соответствии с критериями соглашения — здесь не требуется никаких специальных действий, связанных с цепью поставок ИКТ;

2) обеспечивать помощь приобретающей стороне в сопровождении поставленной продукции или услуги согласно соглашению — здесь не требуется никаких специальных действий, связанных с цепью поставок ИКТ;

е) закрывать соглашение:

1) принимать и подтверждать оплату или другое согласованное действие — здесь не требуется никаких специальных действий, связанных с цепью поставок ИКТ;

2) передавать ответственность за продукцию или услугу приобретающей стороне или другой стороне, как это предписано соглашением, чтобы обеспечить закрытие соглашения, — здесь не требуется никаких специальных действий, связанных с цепью поставок ИКТ;

3) обеспечивать выполнение или поддержание согласованных мер безопасности после прекращения действия соглашения.

5.2 Процессы организационного обеспечения проекта

Процессы организационного обеспечения проекта направлены на обеспечение того, чтобы ресурсы, необходимые для реализации проекта, удовлетворяли потребностям и ожиданиям заинтересованных сторон организации.

Процессы организационного обеспечения проекта создают среду, в которой эти проекты осуществляются. Если конкретно не оговорено, процессы применимы как к приобретающим сторонам, так и к поставщикам.

Дополнительные специальные рекомендации относительно процессов организационного обеспечения проекта см. в ГОСТ Р ИСО/МЭК 27002. Сопоставление положений настоящего подраздела с мерами обеспечения информационной безопасности, рекомендуемыми ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27004, ГОСТ Р ИСО/МЭК 27005, приведено в приложении А.

5.2.1 Процесс управления моделью жизненного цикла

Целью процесса управления моделью жизненного цикла является определение и обеспечение пригодности политики, процессов жизненного цикла, модели жизненного цикла и процедур для использования организацией. Безопасность цепи поставок ИКТ должна рассматриваться в этом процессе, однако отсутствуют какие-либо конкретные указания в дополнение к тому, что предусмотрено в ГОСТ Р 57193, ГОСТ Р ИСО/МЭК 27036-2.

5.2.2 Процесс управления инфраструктурой

Цель процесса управления инфраструктурой заключается в обеспечении благоприятной инфраструктуры в цепи поставок ИКТ для поддержки приобретающей стороны и поставщиков на протяжении всего жизненного цикла.

В рамках процесса управления инфраструктурой для надлежащего реагирования на риски в области информационной безопасности в цепи поставок ИКТ следует выполнять следующие действия:

а) устанавливать и поддерживать прозрачность в своих процессах, среде функционирования и соответствующих активах для производства или применения продукции или услуг;

б) создавать и поддерживать прозрачность в средах разработки, интеграции и производства, включая инвентаризацию активов;

в) устанавливать процессы физической защиты и возможности для аппаратных компонентов и носителей, в том числе во время доставки, удаления и сопровождения;

г) обеспечивать безопасность хранилища кода, включая размещение всех связанных с кодом активов в защищенных хранилищах исходного кода с контролируемым и проверяемым доступом;

д) обеспечивать безопасность среды проектирования/разработки, включая автоматизированные среды сборки с небольшим числом владельцев и высокой прослеживаемостью действий над сценариями сборки и доступом к файлам кода во время сборки, а также аналогичную защиту для сценариев сборки и для других активов, связанных с кодами (включая верификацию в хранилищах кода);

е) устанавливать программу антивирусной защиты как для разрабатываемого кода, так и для среды функционирования, по крайней мере до уровня, описанного в ГОСТ Р ИСО/МЭК 27002;

ж) реализовывать процессы обмена кодом, обеспечивающие целостность и аутентичность, например, с использованием цифровой подписи, контрольных сумм или хэш-функций;

и) для доставки физических товаров использовать методы и упаковки, допускающие вскрытие.

Примечание — Этот процесс определяет, обеспечивает и поддерживает средства, инструменты и средства связи и информационных технологий, необходимые для деятельности организации в отношении области применения настоящего стандарта.

5.2.3 Процесс управления портфелем проектов

Цель процесса управления портфелем проектов состоит в том, чтобы инициировать и удерживать необходимые, достаточные и пригодные проекты для удовлетворения стратегических целей организации. Приобретающие стороны и поставщики должны учитывать безопасность цепи поставок ИКТ в этом процессе, однако отсутствуют какие-либо конкретные указания в дополнение к тому, что предусмотрено в ГОСТ Р 57193 и ГОСТ Р ИСО/МЭК 27036-2.

5.2.4 Процесс управления человеческими ресурсами

Целью процесса управления человеческими ресурсами является обеспечение организации необходимыми человеческими ресурсами и поддержание их компетентности на уровне, совместимом с бизнес-потребностями. В дополнение к внедрению процесса управления человеческими ресурсами (см. ГОСТ Р 57193) и мер обеспечения безопасности человеческих ресурсов (см. ГОСТ Р ИСО/МЭК 27002) приобретающие стороны и поставщики должны информировать персонал о конкретных вопросах, связанных с поставками ИКТ, и о том, как их решать. В частности, с учетом распределения требований в цепочке поставок ИКТ приобретающим сторонам и поставщикам следует выполнять следующие действия:

а) разрабатывать организационную политику и общие контрактные требования для повышения осведомленности и подготовки кадров по вопросам управления рисками в цепи поставок ИКТ;

б) определять и требовать выполнения функций в рамках всей цепи поставок ИКТ и жизненного цикла системы/элемента для ограничения возможностей и средств, имеющихся в распоряжении отдельных лиц, выполняющих эти функции, которые могут привести к неблагоприятным последствиям;

в) разрабатывать комплексную программу повышения осведомленности и профессиональной подготовки, которая будет способствовать разработке политики и процедур обеспечения безопасности в рамках цепи поставок ИКТ в организации;

г) обучать персонал методам обеспечения качества и информационной безопасности с оценкой угроз и уязвимостей в цепи поставок ИКТ;

д) обучать нанимаемый персонал (например, технический персонал, специалистов по оборудованию и менеджеров изделий) надежным процессам получения элементов/услуг (включая запасные части), включая любые известные отклонения в поставках, которые могут указывать на подделки, злоумышленные действия или проблемы с качеством;

е) обучать разработчиков программного обеспечения использованию методов безопасного кодирования, сокращения числа уязвимостей в поставляемом коде и их важности для реагирования на риски в области информационной безопасности в цепи поставок ИКТ;

ж) устанавливать и обеспечивать соблюдение требований в отношении проверок и оценок безопасности персонала. Эти анализы и оценки должны охватывать персонал, который имеет доступ к элементам, процессам или бизнес-деятельности, позволяющим применять технические знания или понимание бизнес-процессов для получения несанкционированного доступа или доступа к элементам или процессам, которые могут привести к нанесению ущерба или компрометации;

и) определять процессы, с использованием которых осуществляется сбор общей информации о цепи поставок ИКТ, извлечение уроков и обмен накопленным опытом между приобретающей стороной и персоналом поставщиков в рамках соглашения;

к) осуществлять управление авторизацией, контроль доступа и мониторинг процессов с целью своевременного выявления и классификации аномального поведения персонала, которое может привести к неблагоприятным последствиям как для физического, так и для логического доступа в цепи поставок ИКТ;

л) устанавливать и применять требования для присвоения уникальных удостоверений всем лицам (например, учетная запись для входа, идентификатор пользователя), включая требования к тому, при каких обстоятельствах такие предметы могут быть использованы повторно (например, при увольнении сотрудника, изменении имени).

5.2.5 Процесс управления качеством

Цель процесса управления качеством состоит в том, чтобы продукция, услуги и реализация процессов жизненного цикла цепи поставок ИКТ соответствовали целям организации в области качества и обеспечивали удовлетворенность приобретающей стороны.

Для реагирования на риски в области информационной безопасности в цепи поставок ИКТ приобретающим сторонам и поставщикам следует выполнять следующие действия:

а) реализовывать действующую программу управления уязвимостями, как минимум сопоставимую с тем, что описано в ГОСТ Р ИСО/МЭК 27002.

Примечание — Общие мероприятия по управлению уязвимостью рассматриваются в 5.3.4;

б) интегрировать в деятельность по управлению качеством процедуру тестирования на наличие «узких мест» и уязвимостей на протяжении всего жизненного цикла системы, включая анализы проекта, архитектуры и документации и различные виды тестирования, которые программное и аппаратное обеспечение проходит перед поставкой и установкой, а также при каждом обновлении.

Примечание — При необходимости следует рассмотреть вопрос об интеграции в деятельность по управлению качеством процедур тестирования на надежность и устойчивость.

5.3 Процессы технического управления

Процессы технического управления используются для установления и развертывания планов, выполнения планов, оценки фактического достижения и продвижения согласно планам и управления выполнением проектов, включая проекты, охватывающие цепи поставок ИКТ. Если не указано иное, эти процессы применимы как к приобретающим сторонам, так и к поставщикам.

Дополнительные специальные рекомендации относительно процессов технического управления см. в ГОСТ Р ИСО/МЭК 27002. Сопоставление положений настоящего подраздела с мерами обеспечения информационной безопасности, рекомендуемыми ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27004, ГОСТ Р ИСО/МЭК 27005, приведено в приложении А.

5.3.1 Процесс планирования проекта

Цель процесса планирования проекта состоит в том, чтобы разработать и скоординировать эффективные и реально осуществимые планы. Для проектов, связанных с продукцией и услугами в области ИКТ, создаваемыми и поставляемыми по географически распределенным цепям поставок, контролируемым несколькими субъектами, приобретающим сторонам и поставщикам следует учитывать и включать в планы проектов:

а) каким образом потребность в обеспечении безопасности информации приобретающей стороны и поставщика повлияет на планы и графики проектов;

б) любые аспекты управления рисками в области информационной безопасности цепи поставок ИКТ, которые должны быть интегрированы в проектные роли, обязанности, ответственности и полномочия;

в) правовые требования различных юрисдикций, относящиеся к цепи поставок ИКТ;

г) ресурсы, необходимые для обеспечения защиты информации приобретающей стороны и поставщика по всей цепи поставок ИКТ, включая кадровые потребности.

5.3.2 Процесс оценки и контроля проекта

Цель процесса оценки и контроля проекта состоит в том, чтобы обеспечить сбалансированность и выполнимость планов, определить статус проекта, его технического выполнения и реализации процессов, направить выполнение согласно планам и графикам в пределах спроектированных бюджетов для технических задач. В дополнение к действиям и задачам процесса оценки и контроля проекта согласно ГОСТ Р 57193 и ГОСТ Р ИСО/МЭК 27036-2, приобретающая сторона должна периодически проводить аудит соответствия продукции или услуг поставщика, чтобы определить, продолжают ли поставщики соответствовать требованиям приобретающей стороны. Необходимо документирование результатов проверок в отчетах о соответствии предъявляемым требованиям. Периодичность проверок соответствия должна определяться на основе выявленного риска в области безопасности цепи поставок ИКТ и допустимости риска со стороны приобретающей стороны.

5.3.3 Процесс управления решениями

Цель процесса управления решениями состоит в обеспечении структурированной, аналитической основы для объективного определения, характеристики и оценивания множества альтернатив решения в любой точке жизненного цикла и выбора наиболее выгодного направления действий. Приобретающие стороны и поставщики должны учитывать безопасность цепи поставок ИКТ в этом процессе, однако отсутствуют какие-либо конкретные указания в дополнение к тому, что предусмотрено в ГОСТ Р 57193 и ГОСТ Р ИСО/МЭК 27036-2.

5.3.4 Процесс управления рисками

Цель процесса управления рисками состоит в том, чтобы непрерывно идентифицировать, анализировать, реагировать и контролировать риски. В дополнение к внедрению процесса управления рисками в ГОСТ Р 57193 и ГОСТ Р ИСО/МЭК 27036-2 и подходу к управлению рисками, описанному в ГОСТ Р ИСО/МЭК 27005, для реагирования на риски в области информационной безопасности в цепи поставок ИКТ приобретающим сторонам и поставщикам следует выполнять следующие действия:

а) выявлять угрозы, уязвимости и последствия, связанные с продукцией и услугами ИКТ;

б) выявлять и документировать риски в цепи поставок ИКТ, связанные с выявленными угрозами и уязвимостями;

в) определять правовые требования различных юрисдикций, имеющие отношение к цепи поставок ИКТ;

г) определять и выбирать стратегию управления рисками в цепи поставок ИКТ, обусловленными определенными уязвимостями;

д) разграничивать обязанности по снижению рисков в цепи поставок ИКТ между приобретающей стороной и поставщиками;

е) устанавливать процессы доведения информации о рисках до приобретающих сторон и поставщиков;

ж) выявлять эффективность прошлых корректирующих действий поставщиков по всей цепи поставок в отношении других продуктов или услуг и применять их к будущей деятельности;

и) определять основные причины «узких мест» и уязвимостей, выявляемых в ходе разработки, поставки и эксплуатации. При необходимости применять контрмеры и меры по смягчению последствий;

к) осуществлять контроль цепи поставок ИКТ на предмет потенциальных проблем, выявлять и анализировать возникающие в результате этого риски в области информационной безопасности и соответствующим образом обновлять стратегии оценки и реакции на риски.

5.3.5 Процесс управления конфигурацией

Цель управления конфигурацией состоит в том, чтобы управлять и контролировать системные элементы и конфигурации по жизненному циклу. Управление конфигурацией имеет решающее значение для понимания того, какие изменения вносятся в продукцию, системы, элементы продукции и системы, в соответствующую документацию и в саму цепь поставок, включая тех, кто вносит эти изменения. Для обеспечения надлежащего учета проблем, связанных с обеспечением информационной безопасности цепи поставок ИКТ, приобретающим сторонам и поставщикам следует включать в процесс управления конфигурацией, где это целесообразно, следующие действия:

а) контроль доступа и конфигурационных изменений в приложении ко всем аппаратным средствам и элементам оборудования на протяжении всего жизненного цикла, включая проектирование, производство, тестирование, эксплуатацию, сопровождение и списание;

б) контроль доступа и изменений в документации, связанной с продукцией и услугами в части ИКТ;

в) утверждение и управление как логическими, так и физическими изменениями в методах доставки;

г) утверждение изменений и управление изменениями в системах и программном обеспечении, включая исходный код, структуры баз данных и значения настраиваемых параметров;

д) размещение всех соответствующих активов в хранилищах исходного кода, чтобы обеспечить должное внимание к информационной безопасности и контролю доступа;

е) безопасное размещение серверов с хранилищами исходного кода, настройка их по требованиям безопасности (например, с наименьшими необходимыми привилегиями, отключенными сервисами, которые не являются необходимыми) и надлежащая защита этих серверов с учетом критичности размещенного кода;

ж) контроль доступа к хранилищам исходных кодов (включая доступ к любой учетной записи системы) с соблюдением принципа разделения обязанностей и повышением прав доступа только в случае необходимости;

и) управление правами доступа к хранилищам (включая доступ к ответвлениям, рабочим областям или наборам кодов), предоставление привилегий доступа только на основе низких привилегий и обоснования необходимости ознакомления;

к) сохранение изменений в хранилищах кода, включая рассмотрение и утверждение для последующего анализа;

л) ведение записей имен файлов, имени учетной записи лица, регистрирующего файл, отметки времени регистрации и строки, которая была изменена в журналах изменений;

м) управление открытостью всех активов кода, соответствующих продуктам, в том числе разработанным в самой компании и поставщиками;

н) установление и сохранение цепи ответственного хранения для каждого конфигурационного элемента с использованием заверяющей подписи для кода, проставления времени и других соответствующих способов.

5.3.6 Процесс управления информацией

Цель процесса управления информацией заключается в предоставлении соответствующей своевременной, полной, достоверной и, при необходимости, конфиденциальной информации назначенным сторонам в течение и (в надлежащих случаях) после завершения жизненного цикла цепи поставок ИКТ. Под информацией подразумевается техническая, проектная, организационная

информация, информация соглашений и пользовательская информация. Информация часто получается из записей данных организации, системы, процесса или проекта. Рекомендации относительно процесса управления информацией см. в ГОСТ Р ИСО/МЭК 27002.

5.3.7 Процесс измерения

Цель процесса измерения заключается в сборе, анализе и представлении данных, относящихся к разработанным продукции и процессам, реализуемым в рамках организации, для поддержки эффективного управления процессами и объективной демонстрации качества продукции и услуг. В процессе измерения отсутствуют аспекты безопасности цепи поставок ИКТ. Рекомендации по измерениям, которые могут использоваться для разработки и осуществления конкретных мер по реагированию на риски в области информационной безопасности в цепи поставок ИКТ, см. в ГОСТ Р ИСО/МЭК 27004.

5.4 Технические процессы

Технические процессы используются для определения требований к системе, преобразования требований в эффективную продукцию, последовательного воспроизводства продукции там, где это необходимо, использования продукции для оказания необходимых услуг, соблюдения условий оказания услуг и удаления продукции, когда это услуги оказаны. Если не указано иное, эти процессы применимы как к приобретающей стороне, так и к поставщикам.

Дополнительные специальные рекомендации относительно технических процессов см. в ГОСТ Р ИСО/МЭК 27002. Сопоставление положений настоящего подраздела с мерами обеспечения информационной безопасности, рекомендуемыми ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27004, ГОСТ Р ИСО/МЭК 27005, приведено в приложении А.

5.4.1 Процесс определения потребностей и требований заинтересованной стороны

Цель процесса определения требований заинтересованной стороны в контексте цепи поставок ИКТ заключается в том, чтобы определить такие требования к продукции или услугам, выполнение которых может обеспечить возможности, необходимые пользователям и другим заинтересованным сторонам системы в определенной окружающей среде при надлежащем управлении рисками в области информационной безопасности.

Примечание — В ГОСТ Р 57193 дополнительно рассмотрен процесс анализа бизнеса или назначения. Приобретающие стороны и поставщики должны учитывать безопасность цепи поставок ИКТ в этом процессе, однако отсутствуют какие-либо конкретные указания в дополнение к действиям, рекомендуемым для процесса определения потребностей и требований заинтересованной стороны, а также к тому, что предусмотрено в ГОСТ Р 57193 и ГОСТ Р ИСО/МЭК 27036-2.

В процессе определения требований заинтересованных сторон приобретающим сторонам и поставщикам продукции и услуг следует выполнять следующие действия:

а) определять и документировать требования к защите информации на основе потребностей приобретающей стороны, требований соответствия имеющейся информации и документации в части оценки рисков и реагирования на риски;

б) анализировать риски и угрозы для поставленных целей и учитывать эти знания при определении требований, связанных с безопасностью поставщиков;

в) определять и документировать требования к целостности информации для поставщиков, включая целостность кодов;

г) определять и документировать требования к целостности системы для поставщиков продукции и услуг ИКТ;

д) определять и документировать требования к доступности информации и систем для поставщиков продукции и услуг ИКТ;

е) определять и документировать требования к конфиденциальности информации для поставщиков продукции и услуг ИКТ;

ж) определять и документировать аспекты информационной безопасности для требований к доставке продукции и услуг ИКТ;

и) определять и документировать последствия нарушений требований информационной безопасности при поставке продукции и услуг ИКТ.

5.4.2 Процесс определения системных требований

В контексте цепи поставок ИКТ цель процесса определения системных требований состоит в том, чтобы преобразовать ориентированное на пользователя представление заинтересованных сторон о желательных возможностях системы в техническое представление решения, которое

удовлетворит эксплуатационные потребности пользователя при надлежащем управлении рисками в области информационной безопасности. Этот процесс создает ряд количественно оцениваемых системных требований, которые для поставщика задают характеристики, атрибуты, функциональные эксплуатационные возможности, которыми система должна обладать для удовлетворения требований заинтересованных сторон.

Примечание — В ГОСТ Р 57193 дополнительно рассмотрены процесс определения проекта и процесс системного анализа. Приобретающие стороны и поставщики должны учитывать безопасность цепи поставок ИКТ в этом процессе, однако отсутствуют какие-либо конкретные указания в дополнение к действиям, рекомендуемым для процесса определения системных требований, а также к тому, что предусмотрено в ГОСТ Р 57193 и ГОСТ Р ИСО/МЭК 27036-2.

В процессе определения системных требований приобретающим сторонам и поставщикам продукции и услуг следует выполнять следующие действия:

а) обеспечивать присвоение элементам различной степени критичности в зависимости от назначения и использования каждого из них;

б) включать рассмотрение и оценку рисков в цепи поставок ИКТ во все управленческие, функциональные и технические требования и бизнес-процессы для защиты элементов, процессов, требований и деловой практики от нарушений конфиденциальности, целостности и доступности информации;

в) при необходимости включать критерии проектирования в защищенном исполнении во все соответствующие технические требования, чтобы получать варианты проектирования элементов, процессов и систем, которые обеспечивают конфиденциальность, целостность и доступность информации в приложении к возможностям функционирования и производительности элемента и системы;

г) обеспечивать защиту требований и поддерживающей документации в цепи поставок ИКТ от таких компрометирующего воздействия или доступа, которые могут привести к потере конфиденциальности, целостности или доступности информации для элементов и системы;

д) осуществлять контроль и переоценку изменяющихся технических требований и корректировать, следуя утвержденным процедурам управления изменениями, требования к защите критических элементов и процессов на протяжении всего жизненного цикла;

е) определять функциональные концепции и связанные с ними сценарии для случаев ненадлежащего использования и злоупотреблений.

5.4.3 Процесс определения архитектуры

Цель процесса определения архитектуры в контексте цепи поставок ИКТ состоит в том, чтобы синтезировать решение, удовлетворяющее системным требованиям, при надлежащем управлении рисками в области информационной безопасности.

Примечание — В ГОСТ Р 57193 дополнительно рассмотрен процесс определения проекта. Приобретающие стороны и поставщики должны учитывать безопасность цепи поставок ИКТ в этом процессе, однако отсутствуют какие-либо конкретные указания в дополнение к действиям, рекомендуемым для процесса определения архитектуры, а также к тому, что предусмотрено в ГОСТ Р 57193 и ГОСТ Р ИСО/МЭК 27036-2.

В процессе определения архитектуры приобретающим сторонам и поставщикам продукции и услуг следует выполнять следующие действия:

а) использовать методы проектирования в защищенном исполнении для предупреждения возможных способов ненадлежащего использования и злоупотребления продукцией или услугой ИКТ или для защиты продукции и/или системы от такого использования. При этом следует убедиться, что архитектура и проект предусматривают предполагаемые и непреднамеренные сценарии использования. Следует выбирать и реализовывать проекты на основе использования допустимых рисков, принимаемых приобретающей стороной, если не удалось их полностью устранить;

б) ограничивать число критических элементов, их размеры и привилегии;

в) снижать сложность в проектировании, производственных процессах и в реализации проекта. Следует учитывать, что сложность имеет множество негативных последствий, включая приложение таких усилий, которые, в свою очередь, могут вызвать проблемы с конфиденциальностью, целостностью или доступностью информации, каскадные сбои из-за плотного соединения элементов или препятствия для анализа первопричин сбоев и инцидентов;

г) использовать механизмы безопасности или меры обеспечения безопасности для сокращения возможностей реализации уязвимостей в цепи поставок ИКТ. Примерами таких механизмов и

мер выступают шифрование, контроль доступа, управление идентификацией, меры обнаружения вредоносных программ или несанкционированного доступа;

д) изолировать элементы (используя такие методы, как виртуальные машины, карантины, решетки, изолированные среды и односторонние шлюзы) для уменьшения ущерба, который один элемент может нанести другому;

е) проектировать контрмеры и меры по смягчению последствий потенциального использования «узких мест» и уязвимостей в ИКТ, а также проектировать элементы для включения методов программирования или конфигурирования (но не ограничиваясь этим);

ж) использовать возможность настройки повышенной изоляции системы или системного элемента, даже если это ухудшает возможности системы (например, при противодействии атакам до тех пор, пока это приемлемо);

и) проектировать элементы так, чтобы выдержать критичные отклонения во входных сигналах (например, чрезмерного напряжения тока, отклонений от приемлемых диапазонов значений и т. д.);

к) проектировать элементы таким образом, чтобы их было трудно отключить, и, если они отключены, использовать методы уведомления, такие как контрольные журналы, доказательства несанкционированного доступа или сигналы тревоги;

л) проектировать механизмы доставки во избежание воздействия или доступа к системе и процессам доставки элементов, а также использовать их в процессе доставки;

м) при необходимости включать отказоустойчивые/резервные или альтернативные системы и элементы системы и обеспечивать их функционирование таким образом, чтобы отказоустойчивые и резервные механизмы не подвергались отказам в общем режиме;

н) определять и/или использовать основанные на стандартах технические интерфейсы и требования к процессам для предоставления вариантов модификации процессов или модификации/замены элементов в случае возникновения компрометации в цепи поставок;

п) проектировать соответствующие меры валидации, которые будут использоваться при реализации и функционировании.

5.4.4 Процесс реализации

Цель процесса реализации состоит в том, чтобы реализовать заданный системный элемент. Для реагирования на риски в области информационной безопасности в цепи поставок ИКТ в процессе реализации приобретающим сторонам и поставщикам продукции и услуг следует выполнять следующие действия:

а) реализовывать архитектуру и проект, учитывающие связанные с цепью поставок ИКТ требования к продукции и услугам;

б) выявлять отклонения от требований, связанных с цепью поставок ИКТ, осуществлять соответствующие меры по смягчению последствий и документировать соответствующую информацию;

в) реализовывать, когда это возможно и целесообразно, аппаратное и программное обеспечение с использованием языков программирования, которые позволяют избежать изначально небезопасных конструкций кодирования. Это позволит уменьшить вероятность возникновения «узких мест» и компрометации, связанных с цепью поставок ИКТ;

г) выявлять и внедрять стандарты интерфейса везде, где это практически возможно, для содействия устойчивости системы и элементов и возможности повторного использования элементов;

д) осуществлять валидацию процесса реализации на соответствующих и определенных этапах с использованием разработанных проверочных тестов, таких как:

1) использование различных методов тестирования, включая фаззинг-тестирование, статический анализ и динамическое тестирование для выявления и устранения «узких мест» и уязвимостей в программном обеспечении;

2) использование положительных и соответствующих отрицательных тестов для верификации того, что система или элемент работают в соответствии с требованиями и без дополнительной функциональности;

3) контроль неожиданного или нежелательного поведения во время тестирования, такого как поведение сети (например, неожиданный «звонок домой» или открытие сетевого порта), поведение файловой системы (например, чтение или запись информации в неожиданные файлы/каталоги), условия гонки и взаимоблокировки;

е) осуществлять защиту доступа к сценариям тестирования и результатам, хранить сценарии тестирования и результаты в системе управления версиями и осуществлять их защиту аналогично защите исходного кода и сценариев тестирования;

ж) обеспечивать наличие требуемых элементов и продолжение поставок в случае компрометации системы/элемента за счет разнообразия поставок (особенно по товарным функциям или в случае компрометации или нарушения механизмов поставки);

и) обеспечивать удаление или отключение любых ненужных функций, распространенных в коммерческих готовых продуктах, которые предназначены для поддержки нескольких приложений или целей. Эти функции, если оставить их активными, могут разрешить несанкционированный доступ или воздействие на систему или выполнение функции, которая снижает доступность других функций;

к) документировать продукцию и/или элементы, специфичные для реализации в соответствии с соглашением.

5.4.5 Процесс комплексирования

Цель процесса комплексирования состоит в том, чтобы создать из множества системных элементов систему (продукт или услугу), которая отвечает системным требованиям, архитектуре и проекту. Для реагирования на риски в области информационной безопасности в цепочке поставок ИКТ в процессе комплексирования приобретающим сторонам и поставщикам продукции и услуг следует выполнять следующие действия:

а) осуществлять соответствующие мероприятия по 5.4.4 для комплексирования с существующими системами;

б) разрабатывать документацию о том, как осуществляются действия, предусмотренные 5.4.4, в ходе комплексирования, и о тех комплексируемых системах, которые существовали до реализации.

5.4.6 Процесс верификации

Целью процесса верификации является обеспечение объективных доказательств того, что системный элемент или система выполняют заданные требования и обладают заданными характеристиками. Сюда следует включать верификацию информации, существовавшей до приобретения, которой обменивались поставщик и приобретающая сторона, и разработку требований к верификации на основе использования данных 5.2—5.4.

Для реагирования на риски в области информационной безопасности в цепи поставок ИКТ в процессе верификации поставщикам продукции и услуг следует выполнять следующие действия:

а) осуществлять верификацию и валидацию, подтверждающие, что требования безопасности в цепи поставок ИКТ были выполнены;

б) осуществлять верификацию того, что деятельность по поддержке поставщиков согласуется с целями обеспечения безопасности информации и продукции для приобретающей стороны;

в) осуществлять верификацию того, что у поставщика существуют достаточные процедуры обеспечения требований безопасности и персонал обучен их применению;

г) осуществлять верификацию того, что документация поставщика по возможностям и функциям безопасности связана с функциями продукции в части архитектуры, проекта, требований, кодов, тестов и результатов тестирования;

д) осуществлять верификацию того, что поставщик проводит действия по верификации и валидации размещения и функционирования средств обеспечения безопасности согласно их назначению, а также их соответствия требованиям приобретающей стороны;

е) осуществлять верификацию того, что между организациями поддерживается цепь поставок;

ж) осуществлять оценку и верификацию кода с использованием различных инструментариев и методов, таких как экспертные обзоры, ручные проверки кода, статический анализ кода, динамический анализ кода, анализ двоичного кода, инструментарии покрытия кода;

и) осуществлять сканирование на предмет выявления уязвимостей сетевых приложений и веб-приложений;

к) осуществлять сканирование на предмет выявления вредоносных программ;

л) использовать инструментарии для валидации соответствия;

м) проводить стресс-тестирование;

н) анализировать аттестаты или сертификаты, предоставляемые поставщиками:

1) в отношении заявлений поставщиков о соответствии требованиям безопасности или бизнес-процедур, целостности продукции или цепи поставок;

2) в отношении награды конкретного продукта для оценки соответствия требованиям к риску приобретающей стороны или пригодности продукции к определенному назначению относительно предполагаемого использования приобретающей стороной.

5.4.7 Процесс передачи

Целью процесса передачи является установление возможности системы к функционированию согласно заданным требованиям заинтересованных сторон в эксплуатационной среде.

Для реагирования на конкретные риски в области информационной безопасности в цепи поставок ИКТ в рамках процесса передачи приобретающим сторонам следует выполнять следующие действия:

а) включать в методы и процессы, связанные с управлением запасами, информацию о порядке запрашивания запасных частей, о соответствующих складских резервах (включая данные о местах их хранения и защите), о порядке получения (чтобы знать, к кому следует обращаться, когда запасы поступают, кто их принимает, где они находятся, и осуществляется ли сверка заказов и поступлений) и о способах учета запасов;

б) включать продукцию и элементы в систему управления запасами организации;

в) разрабатывать механизмы снижения рисков несанкционированного доступа к продукции или услугам в процессе доставки;

г) осуществлять процессы доставки для предполагаемых логической и физической передач и получения элементов, что должен выполнять уполномоченный персонал;

д) устанавливать неразрушающие методы или механизмы для определения наличия несанкционированного доступа на протяжении всего процесса доставки;

е) предусматривать приемлемые уровни информационной безопасности и качества для контроля логической доставки продукции и услуг, требующих загрузки с утвержденных, усиленных верификацией сайтов. Учитывать на протяжении всей доставки востребованное шифрование элементов (для программного обеспечения, программных исправлений и т. д.) при их передаче и хранении;

ж) устанавливать процесс и возможности для защиты программной продукции от вредоносных программ;

и) устанавливать процесс и возможности для верификации таких меток, как цифровые подписи и голограммные ярлыки для критических элементов.

Для реагирования на конкретные риски в области информационной безопасности в цепи поставок ИКТ в рамках процесса передачи поставщикам следует выполнять следующие действия:

а) устанавливать процесс и возможности для защиты программной продукции от вредоносных программ;

б) рассматривать элементы шифрования (для программного обеспечения, программных исправлений и т. д.) при передаче и при доставке в другое время;

в) для снижения рисков подделки и обеспечения возможности верификации приобретающей стороной использовать такие способы, как трудно поддающиеся подделке метки (например, цифровые подписи и голографические ярлыки) для критических элементов, цифровые метки, включающие авторизацию поставщика, криптографически подписывающие программные компоненты, использование цифровых хэш-функций;

г) развертывать специальные процессы как для оперативной (он-лайн), так и для автономной (офф-лайн) доставки программного обеспечения. Предоставлять информацию приобретающей стороне о подписании кода и контрольных суммах;

д) устанавливать процесс доставки продукции таким образом, чтобы приобретающая сторона могла подтвердить, что продукт поступает от конкретного поставщика;

е) устанавливать противовзломные механизмы для предотвращения и обнаружения, включая защиту от подделки и несанкционированного вскрытия упаковки (например, тейп-ленты или пломбы). Такие защитные элементы не должны быть легко удаляемыми и заменяемыми без оставления признаков несанкционированных действий.

5.4.8 Процесс валидации (аттестации)

Цель процесса валидации в контексте цепи поставок ИКТ заключается в предоставлении объективных доказательств того, что продукция и услуги соответствуют требованиям заинтересованных сторон, обеспечивая их целевое использование в заданной эксплуатационной среде.

Процесс валидации должен включать в себя определение того, являются ли полученный продукт или услуга подлинными и неизменными на основе их описания или требований поставщика, а также соглашение между приобретающей стороной и поставщиком. Процесс также должен включать разработку тестов, которые обеспечивают валидацию на протяжении всего периода использования продукции приобретающей стороной. В частности, для реагирования на конкретные риски в области

информационной безопасности в цепи поставок ИКТ в рамках процесса валидации приобретающим сторонам следует выполнять следующие действия:

а) осуществлять верификацию и валидацию того, что требования безопасности цепи поставок ИКТ были выполнены;

б) там, где это уместно, разрабатывать процессы для использования методов изготовителя оригинального оборудования, инструментариев валидации продукции и программного обеспечения, которые являются бесконтактными и могут обнаруживать подделку или несанкционированное вмешательство в содержимое продукта;

в) проводить испытания при получении, а также на этапах разработки и эксплуатации системы. Пытаться обнаружить подделку или несанкционированное вмешательство в содержимое продукта, для чего:

1) проводить верификацию аппаратного и программного обеспечения на подлинные компоненты с использованием рекомендаций и инструментариев, предоставляемых поставщиком, третьими сторонами или приобретающей стороной (например, для ручной проверки кода);

2) проводить проверки на наличие вредоносных программ;

3) проводить сканирование уязвимостей;

г) использовать документацию на продукцию и планы приобретающей стороны для идентификации и тестирования критических компонентов;

д) проводить оценку и верификацию кода с использованием различных инструментариев и методов, таких как статический анализ кода, динамический анализ кода, анализ двоичного кода, инструментарии покрытия кода;

е) проводить стресс-тестирование;

ж) использовать инструментарии для сбора доказательств об изменениях, возникающих в результате операций удаленного сопровождения продукции.

5.4.9 Процесс функционирования

Цель процесса функционирования заключается в использовании системы для выполнения заданных функций.

Для реагирования на конкретные риски в области информационной безопасности в цепи поставок ИКТ в рамках процесса функционирования приобретающим сторонам и поставщикам следует выполнять следующие действия:

а) поставлять элементы («безопасные по умолчанию») на уровне, соответствующем требованиям приобретающей стороны;

б) включать в эксплуатационные требования к системе соответствующие действия по комплексированию системы и расширению пользовательского кода в рамках усилий по обновлению и сопровождению;

в) выполнять все применимые действия по обеспечению информационной безопасности и реализовывать применимые требования к информационной безопасности в процессе функционирования.

5.4.10 Процесс сопровождения

Цель процесса сопровождения в контексте цепи поставок ИКТ заключается в поддержании способности системы и ее компонентов предоставлять услуги при надлежащем управлении рисками в области информационной безопасности.

Для реагирования на конкретные риски в области информационной безопасности в цепи поставок ИКТ в рамках процесса сопровождения приобретающим сторонам и поставщикам следует выполнять следующие действия:

а) использовать положения о закупках для снижения рисков в цепи поставок ИКТ в рамках официальных соглашений о техническом обслуживании и сопровождении с поставщиками;

б) при приобретении элементов изготовителя оригинального оборудования, включая восстанавливаемые элементы, устанавливать договорные отношения с производителем или первоначальным создателем, который обеспечивает проверенную компетентную поддержку (там, где это возможно);

в) рассматривать возможность заблаговременной закупки и инвентаризации запасных частей, пока они широко доступны, поддаются проверке и могут быть установлены обученным и хорошо осведомленным авторизованным персоналом;

г) учитывать риски, связанные с тем, что обученный и хорошо осведомленный авторизованный персонал может оказаться недоступным, особенно в конце срока службы элемента;

д) учитывать риски в цепи поставок ИКТ при приобретении запасных компонентов или дополнений/модификаций/модернизаций, особенно если они не проходят через традиционные процессы приобретения, которые изучают риски в цепи поставок;

е) отдавать предпочтение формализованным соглашениям о сопровождении/техническом обслуживании, где это возможно, например использовать определенных или квалифицированных поставщиков запасных частей, представлять полный отчет об изменениях, выполненных во время технического обслуживания (например, журнал аудита или журнал изменений), анализировать изменения, внесенные во время технического обслуживания;

ж) заключать и осуществлять соглашения о компетентной и надлежащей поддержке, включая поддержку восстанавливаемых и/или утилизируемых элементов. Рекомендуется также озаботиться тем, чтобы потребовать от первоначального производителя сертификаты соответствия на оригинальное оборудование;

и) определять методы верификацию того, что обслуживающий персонал аутентифицирован и уполномочен для выполнения работ по сопровождению, необходимых в данный момент;

к) разрабатывать и реализовывать подход к сбору и обработке сообщений об аномалиях в цепи поставок ИКТ при эксплуатации;

л) следить за состоянием бизнеса поставщика, в том числе за тем, является ли он кандидатом на слияние и поглощение или испытывает финансовые трудности;

м) реализовывать и применять политику в отношении обновлений программного обеспечения и управления исправлениями;

н) создавать достаточный запас надежных запасных частей и обеспечивать техническое обслуживание на срок службы элементов;

п) сохранять документацию для любого элемента в процессе эксплуатации, который больше не поддерживается поставщиком.

5.4.11 Процесс изъятия и списания

Цель процесса изъятия и списания в цепи поставок ИКТ заключается в прекращении существования элементов цепи поставок ИКТ. Изъятие и списание может происходить в любой момент жизненного цикла системы или элемента и включает в себя как электронные, так и неэлектронные носители.

Для реагирования на конкретные риски в области информационной безопасности в цепи поставок ИКТ (в частности риска появления в цепи поставок контрафактной продукции) в рамках процесса изъятия и списания приобретающим сторонам и поставщикам следует выполнять следующие действия:

а) сохранять цепь хранения для элементов, подлежащих изъятию и списанию, чтобы снизить риски компрометации, например личных идентифицируемых данных или интеллектуальной собственности;

б) поощрять выбор элементов, которые могут быть изъяты и списаны таким образом, чтобы не подвергать опасности защищаемую информацию, например элементов, которые позволяют выгружать данные перед изъятием и списанием, или элементов, которые легко стирать перед утилизацией;

в) запрещать передачу или распространение конфиденциальных данных или критичных элементов приобретающей стороны несанкционированным или неопределенным сторонам в ходе действий по изъятию и списанию;

г) при необходимости проведения криминалистической экспертизы или последующего сопоставления для выявления подделок хранить элементы для утилизации в специальном хранилище и поддерживать цепочку хранения,

д) осуществлять процедуры безопасного и постоянного уничтожения элементов;

е) привлекать надежный, обученный персонал службы изъятия и списания и устанавливать требования к процедурам, соответствующим политике изъятия и списания. Верифицировать соблюдение процедур с использованием соответствующих оценок.

Приложение А
(справочное)

Сопоставление мер раздела 5 настоящего стандарта с мерами, рекомендуемыми другими стандартами в области информационной безопасности

В таблице А.1 приведены сведения о сопоставлении мер раздела 5 настоящего стандарта с мерами обеспечения информационной безопасности, рекомендуемыми ГОСТ Р ИСО/МЭК 27002, ГОСТ Р ИСО/МЭК 27004, ГОСТ Р ИСО/МЭК 27005.

Таблица А.1

Раздел 5 настоящего стандарта	ГОСТ Р ИСО/МЭК 27002[1], ГОСТ Р ИСО/МЭК 27004, ГОСТ Р ИСО/МЭК 27005
5 Безопасность цепи поставок информационных и коммуникационных технологий в процессах жизненного цикла	См. далее по каждому процессу
5.1 Процессы соглашения 5.1.1 Процесс приобретения 5.1.2 Процесс поставки	5 Политика информационной безопасности 6 Организация деятельности по информационной безопасности 15 Взаимоотношения с поставщиками 18 Соответствие
5.2 Процессы организационного обеспечения проектов	См. сопоставление по процессам 5.2.1—5.2.5
5.2.1 Процесс управления моделью жизненного цикла	Нет
5.2.2 Процесс управления инфраструктурой	8 Менеджмент активов 9 Управление доступом 10 Криптография 11 Физическая безопасность и защита от воздействия окружающей среды 12 Безопасность при эксплуатации 13 Безопасность коммуникаций 16 Менеджмент инцидентов информационной безопасности 17 Аспекты информационной безопасности в рамках менеджмента непрерывности деятельности организации
5.2.3 Процесс управления портфелем проектов	Нет
5.2.4 Процесс управления человеческими ресурсами	7 Безопасность, связанная с персоналом
5.2.5 Процесс управления качеством	14.2 Безопасность в процессах разработки и поддержки 14.3 Тестовые данные
5.3 Процессы технического управления	См. сопоставление по процессам 5.3.1—5.3.7
5.3.1 Процесс планирования проекта	Нет
5.3.2 Процесс оценки и контроля проекта	Нет
5.3.3 Процесс управления решениями	Нет
5.3.4 Процесс управления рисками	См. ГОСТ Р ИСО/МЭК 27005
5.3.5 Процесс управления конфигурацией	12.1.2 Процесс управления изменениями 14.2.2 Процедуры управления изменениями системы

Окончание таблицы А.1

Раздел 5 настоящего стандарта	ГОСТ Р ИСО/МЭК 27002[1)], ГОСТ Р ИСО/МЭК 27004, ГОСТ Р ИСО/МЭК 27005
5.3.6 Процесс управления информацией	8.2 Категорирование информации 9.1 Требование бизнеса по управлению доступом 10 Криптография 12.3 Резервное копирование 13.2.1 Политики и процедуры передачи информации
5.3.7 Процесс измерения	См. ГОСТ Р ИСО/МЭК 27004
5.4 Технические процессы	См. сопоставление по процессам 5.4.1—5.4.11
5.4.1 Процесс определения потребностей и требований заинтересованной стороны	14.1 Требования к безопасности информационных систем
5.4.2 Процесс определения системных требований	14.1 Требования к безопасности информационных систем
5.4.3 Процесс определения архитектуры	Нет
5.4.4 Процесс реализации	14.2 Безопасность в процессах разработки и поддержки
5.4.5 Процесс комплексирования	14.2 Безопасность в процессах разработки и поддержки
5.4.6 Процесс верификации	14.2 Безопасность в процессах разработки и поддержки 14.3 Тестовые данные
5.4.7 Процесс передачи	14.2.8 Тестирование безопасности системы
5.4.8 Процесс валидации (аттестации)	14.2 Безопасность в процессах разработки и поддержки 14.3 Тестовые данные
5.4.9 Процесс функционирования	8 Менеджмент активов 9 Управление доступом 10 Криптография 12 Безопасность при эксплуатации 13 Безопасность коммуникаций 16 Менеджмент инцидентов информационной безопасности 17 Аспекты информационной безопасности в рамках менеджмента непрерывности деятельности организации 18 Соответствие
5.4.10 Процесс сопровождения	8.3 Обращение с носителями информации 13 Безопасность коммуникаций 17 Аспекты информационной безопасности в рамках менеджмента непрерывности деятельности организации
5.4.11 Процесс изъятия и списания	8 Менеджмент активов 13.2 Передача информации

[1)] По состоянию на 2020 г. взамен ГОСТ Р ИСО/МЭК 27002—2013 разрабатывается новый стандарт.

УДК 006.34:004.056:004.056.5:004.056.53:006.354 ОКС 35.020

Ключевые слова: информационная безопасность, информационные и коммуникационные технологии, методы и средства обеспечения безопасности, поставщик, приобретающая сторона, риск, система, цепь поставок

Редактор *Л.И. Нахимова*
Технический редактор *В.Н. Прусакова*
Корректор *Е.Д. Дульнева*
Компьютерная верстка *И.А. Налейкиной*

Сдано в набор 30.11.2020. Подписано в печать 16.12.2020. Формат 60×84 1/8. Гарнитура Ариал.
Усл. печ. л. 3,26. Уч.-изд. л. 2,64.
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 gost.e-ecolog.ru

gost.e-ecolog.ru