ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27017— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Правила применения мер обеспечения информационной безопасности на основе ИСО/МЭК 27002 при использовании облачных служб

(ISO/IEC 27017:2015, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

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

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 19 мая 2021 г. № 389-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27017:2015 «Информационные технологии. Методы и средства обеспечения безопасности. Правила применения мер обеспечения информационной безопасности на основе ИСО/МЭК 27002 при использовании облачных служб» (ISO/IEC 27017:2015 «Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services», IDT).

ИСО/МЭК 27017 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 ссылочных международных стандартов соответствующие им национальные и межгосударственные стандарты, сведения о которых приведены в дополнительном приложении ДА

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые положения международного стандарта, указанного в пункте 4, могут являться объектом патентных прав. ИСО и 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

Руководящие принципы, содержащиеся в настоящем стандарте, дополняют руководящие принципы, приведенные в ИСО/МЭК 27002.

В частности, в настоящем стандарте представлено руководство по реализации мер обеспечения информационной безопасности (ИБ) для потребителей и поставщиков облачных служб. Некоторые руководящие принципы предназначены для потребителей облачных служб, внедряющих меры обеспечения ИБ, а другие — для поставщиков облачных служб с целью поддержки реализации этих мер. Выбор соответствующих мер обеспечения ИБ и применение предоставленных рекомендаций по их реализации будут зависеть от оценки рисков, а также правовых, договорных, нормативных и иных требований ИБ в сфере облачных вычислений[1)].

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

Федеральное агентство
по техническому регулированию
и метрологии
Федеральное агентство
по техническому регулированию
и метрологии

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Правила применения мер обеспечения информационной безопасности на основе ИСО/МЭК 27002 при использовании облачных служб

Information technology. Security techniques. Code of practice for information security controls based on ISO/IEC 27002 for cloud services

Дата введения — 2021—11—30

1 Область применения

В настоящем стандарте приведены руководящие указания по обеспечению ИБ, применимые к облачным службам, благодаря использованию:

- дополнительного руководства по реализации соответствующих мер обеспечения ИБ, приведенных в ИСО/МЭК 27002;
- дополнительных мер обеспечения ИБ, а также соответствующих рекомендаций по их реализации, относящихся непосредственно к облачным службам.

В настоящем стандарте представлено руководство по реализации мер обеспечения ИБ как для потребителей, так и для поставщиков облачных служб.

2 Нормативные ссылки

В настоящем стандарте использованы следующие нормативные ссылки. Для датированных ссылок применяют только указанное издание. Для недатированных — последнее издание (включая все изменения).

2.1 Идентичные стандарты, касающиеся облачных вычислений

ISO/IEC 17788, Information technology — Cloud computing — Overview and Vocabulary (Информационные технологии. Облачные вычисления. Общие положения и терминология)

ISO/IEC 17789, Information technology — Cloud computing — Reference architecture (Информационные технологии. Облачные вычисления. Эталонная архитектура)

2.2 Дополнительные ссылки

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

ISO/IEC 27002:2013, Information technology — Security techniques — Code of practice for information security controls (Информационные технологии. Методы и средства обеспечения безопасности. Свод норм и правил применения мер обеспечения информационной безопасности)

Издание официальное

3 Термины, определения и сокращения

3.1 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 27000, ИСО/МЭК 17788, ИСО/МЭК 17789, а также следующие термины с соответствующими определениями:

3.1.1 **способность** (capability): Качество, характеризующее способность осуществлять данный вид деятельности.

[ИСО 19440, статья 3.1.5]

3.1.2 **компрометация данных** (data breach): Нарушение безопасности, которое приводит к случайному или незаконному разрушению, потере, изменению, несанкционированному раскрытию или доступу к защищаемым данным, передаваемым, хранимым или иным образом обрабатываемым.

[ИСО/МЭК 27040, статья 3.7]

3.1.3 **защищенная совместно арендуемая среда** (secure multi-tenancy): Совместно арендуемая среда, в которой используются меры ИБ, обеспечивающие непосредственную защиту от компрометации данных (3.1.2), и осуществляется проверка указанных мер с целью надлежащей защиты

Примечания

1 Совместно арендуемая среда является защищенной, если уровень риска отдельного арендатора не превышает уровня его риска в одной выделенной арендной среде.

2 В наиболее защищенных средах не раскрывается даже личность пользователей.

[ИСО/МЭК 27040, статья 3.39]

3.1.4 **виртуальная машина** (virtual machine): Полная среда, которая поддерживает выполнение гостевого программного обеспечения.

Примечание — Виртуальная машина — это полная инкапсуляция виртуального аппаратного обеспечения, виртуальных дисков и связанных с ними метаданных. Виртуальные машины позволяют мультиплексировать возможности базовой физической машины посредством уровня программного обеспечения, называемого гипервизором.

[ИСО/МЭК 17203, статья 3.20]

3.2 Сокращения

В настоящем стандарте применены следующие сокращения:

IaaS — инфраструктура как услуга (Infrastructure as a Service);

PaaS — платформа как услуга (Platform as a Service);

SaaS — программное обеспечение как услуга (Software as a Service);

SLA — соглашение об уровне обслуживания (Service Level Agreement);

ВМ — виртуальная машина;

ПДн — персональные данные.

4 Концепции облачных вычислений

4.1 Обзор

Использование технологии облачных вычислений способствует развитию новых подходов к оценке и снижению рисков ИБ. Это связано со значительными изменениями в техническом проектировании вычислительных ресурсов, их эксплуатации и управлении ими. Настоящий стандарт содержит схожие руководящие принципы по реализации мер обеспечения ИБ в сфере облачных вычислений, основанные на ИСО/МЭК 27002, и предоставляет дополнительные меры для устранения специфичных для облачных служб угроз и рисков ИБ.

Пользователям настоящего стандарта следует обращаться к ИСО/МЭК 27002 (разделы 5—18), в котором содержатся описание мер обеспечения ИБ, рекомендации по их реализации и дополнительная информация. Поскольку ИСО/МЭК 27002 носит универсальный характер, многие меры обеспечения ИБ, рекомендации по их реализации и дополнительная информация применимы организациями как в общем контексте, так и в контексте облачных вычислений. Так, в пункте 6.1.2 «Разделение обязанностей» ИСО/МЭК 27002 предусмотрены меры обеспечения ИБ, которые могут применяться независимо от того, действует ли организация в качестве поставщика облачных служб. Кроме того, на основе этих

мер потребитель облачных служб может определить требования к разделению обязанностей в облачной среде, например разделить обязанности администраторов, клиентов и пользователей облачных служб.

В качестве дополнения к ИСО/МЭК 27002 настоящий стандарт также предоставляет специальные меры обеспечения ИБ в сфере облачных вычислений, руководство по их реализации и дополнительную информацию (подраздел 4.5), которые предназначены для снижения рисков, связанных с техническими и эксплуатационными характеристиками облачных служб (приложение В). Потребители и поставщики облачных служб могут обращаться к ИСО/МЭК 27002 и настоящему стандарту для выбора мер обеспечения ИБ, использования руководства по их реализации, а также добавлять другие меры и средства при необходимости. Этот процесс может быть выполнен путем оценки и обработки рисков в области ИБ в организационной и бизнес-среде, где используются или предоставляются услуги в сфере облачных вычислений (подраздел 4.4).

4.2 Взаимоотношения с поставщиками облачных служб

В разделе 15 «Взаимоотношения с поставщиками» ИСО/МЭК 27002 приведены меры обеспечения ИБ, рекомендации по их реализации и дополнительная информация по управлению ИБ в рамках взаимоотношений с поставщиком. Обеспечение и использование облачных служб представляет собой такие отношения с поставщиком, в которых потребитель облачных служб выступает в качестве приобретателя, а поставщик облачных служб — в качестве поставщика. Таким образом, указанный раздел распространяется на потребителей и поставщиков облачных служб.

Потребители и поставщики облачных служб могут формировать целые цепочки поставок. Например, один поставщик облачных служб предоставляет определенный тип возможностей облака, например тип возможностей инфраструктуры. При этом другой поставщик облачных служб может предоставить другой тип возможностей облака, например тип возможностей приложения. В этом случае второй поставщик является потребителем облачных служб по отношению к первому и поставщиком облачных служб — по отношению к потребителю облачных служб, использующему эту службу. Приведенный пример описывает ситуацию, когда настоящий стандарт применим как к организации, выступающей потребителем, так к поставщику облачных служб. Поскольку потребители и поставщики облачных служб образуют цепочку поставок посредством проектирования и реализации облачных служб, могут быть применимы положения пункта 15.1.3 «Цепочка поставок информационно-коммуникационных технологий» ИСО/МЭК 27002.

ИСО/МЭК 27036 (все части) «Информационная безопасность во взаимоотношениях с поставщиками» содержит подробное руководство по обеспечению ИБ во взаимоотношениях с поставщиком, которое может быть применено как для потребителя, так и для поставщика товаров и услуг. ИСО/МЭК 27036-4 непосредственно касается вопросов безопасности облачных служб в рамках взаимоотношений с поставщиками. Указанный стандарт также применим к потребителям облачных служб, выступающим в качестве приобретателей, и поставщикам облачных служб, выступающим в качестве поставщиков.

4.3 Взаимоотношения между потребителями и поставщиками облачных служб

В среде облачных вычислений данные потребителей облачных служб хранятся, передаются и обрабатываются облачными службами. Таким образом, ИБ облачных служб может оказывать влияние на бизнес-процессы потребителя этих служб. В отсутствие достаточных мер обеспечения ИБ облачными службами потребителю этих служб может потребоваться принять дополнительные меры предосторожности в части обеспечения ИБ.

Прежде чем вступить во взаимоотношения с поставщиком, потребитель облачных служб должен выбрать службу, принимая во внимание возможные расхождения между требованиями потребителя к ИБ, возможностями поставщика и предоставляемыми услугами. После выбора облачной службы потребитель должен осуществлять управление использованием службы таким образом, чтобы соответствовать требованиям к ИБ, предъявляемым к службе. При этом поставщик облачной службы должен обеспечить информационную и техническую поддержку, необходимую для удовлетворения требований к ИБ потребителя облачной службы. Если меры обеспечения ИБ, предоставляемые поставщиком облачной службы, заданы заранее и не могут быть изменены потребителем облачной службы, то для снижения рисков потребителю может потребоваться реализовать собственные дополнительные меры обеспечения ИБ.

4.4 Управление рисками информационной безопасности в облачных службах

Потребители и поставщики облачных служб должны внедрить процессы управления рисками ИБ. Для получения информации о требованиях к управлению рисками в системах менеджмента информационной безопасности (СМИБ) рекомендуется обратиться к ИСО/МЭК 27001, а для получения дополнительного руководства по менеджменту рисков ИБ — к ИСО/МЭК 27005. Для общего понимания менеджмента рисков следует обратиться к ИСО 31000, положения которого соответствуют положениям ИСО/МЭК 27001 и ИСО/МЭК 27005.

В отличие от общей применимости процессов управления рисками ИБ, для технологии облачных вычислений характерны отдельные типы источников риска, в том числе угрозы и уязвимости, связанные с функциональными особенностями этой технологии, такими как сетевое взаимодействие, масштабируемость и эластичность систем, совместное обеспечение услуг, системы самообслуживания, администрирование по требованию, обеспечение услуг между юрисдикциями и ограниченная видимость процессов реализации мер обеспечения ИБ.

В приложении В приводятся ссылки, в которых содержится информация о таких источниках риска и соответствующих рисках при обеспечении и использовании облачных служб.

Меры обеспечения ИБ, касающиеся конкретных источников рисков облачных вычислений, и рекомендации по их реализации приведены в разделах 5—18 и приложении А.

4.5 Структура стандарта

Структура настоящего стандарта аналогична структуре ИСО/МЭК 27002. Настоящий стандарт включает в себя положения ИСО/МЭК 27002 (разделы 5—18) с указанием их применимости в каждом разделе и пункте.

Если цель и мера обеспечения ИБ, определенные в ИСО/МЭК 27002, применимы без необходимости получения какой-либо дополнительной информации, то указывается только ссылка на ИСО/МЭК 27002.

Если в дополнение к указанным целям и мерам обеспечения ИБ из ИСО/МЭК 27002 требуются дополнительные цели и меры из ИСО/МЭК 27002, то они приводятся в приложении А. Если в отношении мер обеспечения ИБ из ИСО/МЭК 27002 или приложения А требуются дополнительные рекомендации по реализации соответствующих мер обеспечения ИБ, то такие рекомендации приводятся под заголовком «Рекомендации по реализации для облачных служб». Руководство приводится в виде одного из следующих типов.

Тип 1 используется в случаях, когда для потребителя и поставщика облачных служб применяются отдельные руководящие принципы.

Тип 2 используется в случаях, когда для потребителя и поставщика облачных служб применяются одни и те же руководящие принципы.

Тип 1

Потребитель облачных служб	Поставщик облачных служб

Тип 2

Потребитель облачных служб	Поставщик облачных служб

Дополнительная информация, которую возможно потребуется учитывать, приводится под заголовком «Дополнительная информация для облачных служб».

5 Политики информационной безопасности

5.1 Руководящие указания в части информационной безопасности

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 5.1).

5.1.1 Политики информационной безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 5.1.1. Также применяются следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен определить отдельную политику, касающуюся вопросов ИБ в сфере облачных вычислений. Политика ИБ в сфере облачных вычислений должна соответствовать допустимым уровням рисков ИБ, принятым в организации в отношении информационных и других активов. При определении политики ИБ в сфере облачных вычислений потребитель облачной службы должен учитывать следующее: - возможность доступа к информации, хранящейся в облачной среде, и управления ею со стороны поставщика облачных служб; - возможность обслуживания активов в облачной среде, например прикладных программ; - возможность выполнения процессов в многопользовательской виртуализированной облачной службе; - пользователей облачных служб и среду, в которой они ее используют; - администраторов облачных служб со стороны потребителя служб (доступ с привилегией); - географическое расположение организации поставщика облачных служб и страны, в которых поставщик может хранить данные о потребителях облачных служб (даже временно)	Поставщик облачных служб должен дополнить свою политику ИБ с учетом вопросов обеспечения и использования облачных служб, учитывая следующее: - базовые требования к ИБ, применимые к проектированию и внедрению облачной службы; - риски, связанные с уполномоченными инсайдерами; - многопользовательскую среду и изоляцию потребителей облачных служб (включая виртуализацию); - доступ к активам потребителя облачных служб для сотрудников поставщика облачных служб; - процедуры контроля доступа, например строгую аутентификацию для административного доступа к облачным службам; - взаимодействие с потребителями облачных служб в процессе управления изменениями; - безопасность виртуализации; - доступ к данным потребителей облачных служб и их защиту; - управление жизненным циклом учетных записей потребителей облачных служб; - информирование о нарушениях и руководящие принципы в области обмена информацией для содействия в процессе расследований и криминалистических исследований

Дополнительная информация для облачных служб

Политика ИБ в сфере облачных вычислений приведена в пункте 5.1.1 ИСО/МЭК 27002 в качестве специализированной политики. Действие политики ИБ организации охватывает ее информационные и бизнес-процессы. Если организация становится потребителем облачных служб, она может определить соответствующую политику при использовании облачных вычислений. В среде облачных вычислений организация может хранить информацию или управлять бизнес-процессами. Требования политики в сфере облачных вычислений соответствуют общим требованиям к ИБ, изложенным в основной политике ИБ.

При этом политика ИБ для предоставления облачных служб охватывает только информационные и бизнес-процессы потребителя облачных служб и не охватывает информационные и бизнес-процессы поставщика облачных служб. Требования к ИБ для обеспечения облачных служб должны соответствовать требованиям потенциальных потребителей облачных служб. В результате такие требования могут не соответствовать требованиям к безопасности информационных и бизнес-процессов поставщика облачных служб. Область применения политики зачастую определяется соответственно с точки зрения службы, а не только организационной структурой или физическим местоположением.

Безопасность виртуализации в сфере облачных вычислений имеет несколько аспектов, включая в себя управление жизненным циклом экземпляров виртуальных машин, хранение и контроль доступа для виртуализированных образов, обработку неактивных или отключенных экземпляров ВМ, мгновенных снимков, защиту гипервизоров и средства управления безопасностью использования порталов самообслуживания.

5.1.2 Пересмотр политик информационной безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 5.1.2.

6 Организация деятельности по информационной безопасности

6.1 Внутренняя организация деятельности по обеспечению информационной безопасности

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 6.1).

6.1.1 Роли и обязанности по обеспечению информационной безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 6.1.1. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен согласовать с поставщиком облачных служб соответствующее разделение ролей и обязанностей в области ИБ и подтвердить, что он может исполнять назначенные ему роли и обязанности. Роли по обеспечению ИБ и обязанности обеих сторон должны быть задокументированы в соглашении. Потребитель облачных служб должен определить порядок взаимодействия с функцией клиентской поддержки и обслуживания поставщика облачных служб и управлять этим взаимодействием	Поставщик облачных служб должен согласовать и задокументировать соответствующее разделение ролей и обязанностей по обеспечению ИБ со своими потребителями облачных служб, поставщиками облачных служб и другими поставщиками

Дополнительная информация для облачных служб

Хотя обязанности определяются взаимоотношениями сторон, ответственность за решение об использовании облачных служб несет потребитель. Такое решение должно приниматься в соответствии с ролями и обязанностями, определенными в организации потребителя облачных служб. Поставщик облачных служб несет ответственность за обеспечение ИБ, предусмотренной в соглашении о предоставлении облачной службы. Реализация и обеспечение ИБ должны осуществляться в соответствии с ролями и обязанностями, определенными в организации поставщика облачных служб.

Неоднозначность в определении ролей, а также в определении и разделении обязанностей, связанных с такими вопросами, как владение данными, управление доступом и обслуживание инфраструктуры, могут привести к возникновению коммерческих и юридических споров, особенно при работе с третьими сторонами.

Данные и файлы в системах поставщика облачных служб, создаваемые или изменяемые в процессе использования облачных служб, могут иметь решающее значение для обеспечения безопасной и бесперебойной работы службы, а также ее восстановления в случае сбоев. Права собственности на все активы, а также стороны, ответственные за соответствующие операции, такие как резервное копирование и восстановление данных, должны быть определены и задокументированы. В противном случае существует риск утечки данных в результате того, что поставщик облачных служб будет полагать, что эти критически важные задачи выполняет потребитель облачных служб (или наоборот).

6.1.2 Разделение обязанностей

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 6.1.2.

6.1.3 Взаимодействие с органами власти

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 6.1.3. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен определить инстанции, имеющие отношение к совместным операциям потребителя и поставщика облачных служб	Поставщик облачных служб должен информировать потребителя облачных служб о географическом расположении организации поставщика облачных служб и странах, в которых поставщик может хранить данные потребителя облачных служб

Дополнительная информация для облачных служб

Информация о географическом расположении мест, в которых могут храниться, обрабатываться или передаваться данные потребителя облачных служб, может помочь ему в определении контролирующих инстанций и юрисдикций.

6.1.4 Взаимодействие с профессиональными сообществами

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 6.1.4.

6.1.5 Информационная безопасность при управлении проектом

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 6.1.5.

6.2 Мобильные устройства и дистанционная работа

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 6.2).

6.2.1 Политика использования мобильных устройств

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 6.2.1.

6.2.2 Дистанционная работа

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 6.2.2.

7 Безопасность, связанная с персоналом

7.1 При приеме на работу

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 7.1).

7.1.1 Поверка

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 7.1.1.

7.1.2 Правила и условия работы

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 7.1.2.

7.2 Во время работы

Применяется цель, определенная в ИСО/МЭК (подраздел 7.2).

7.2.1 Обязанности руководства организации

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 7.2.1.

7.2.2 Осведомленность, обучение и практическая подготовка (тренинги) в области информационной безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 7.2.2. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен включить в свои информационно-просветительские и учебные программы по облачным вычислениям для руководителей, менеджеров, администраторов, интеграторов и пользователей облачных служб (в том числе соответствующих сотрудников и подрядчиков) вопросы, касающиеся следующего: - стандартов и процедур использования облачных служб; - рисков ИБ, связанных с облачными службами, и способов управления этими рисками; - рисков системной и сетевой среды при использовании облачных служб; - применимых нормативно-правовых вопросов. Следует обеспечить прохождение информационно-просветительских и учебных программ по вопросам облачных вычислений руководством и руководителями контролирующих подразделений, в том числе бизнес-подразделений. Это способствует эффективной координации действий по обеспечению ИБ	Поставщик облачных служб должен обеспечивать прохождение своими сотрудниками информационно-просветительских и учебных программ, а также требовать от своих подрядчиков обучения в отношении надлежащего обращения с данными потребителей облачных служб и данными, полученными из облачных служб. Такие данные могут содержать конфиденциальную информацию потребителя облачных служб, или в отношении такой информации могут действовать определенные ограничения, в том числе нормативные, в отношении доступа и использования поставщиком облачных служб

7.2.3 Дисциплинарный процесс

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 7.2.3.

7.3 Увольнение и смена места работы

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 7.3).

7.3.1 Прекращение или изменение трудовых обязанностей

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 7.3.1.

8 Менеджмент активов

8.1 Ответственность за активы

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 8).

8.1.1 Инвентаризация активов

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 8.1.1. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Инвентаризация активов потребителя облачных служб должна учитывать информацию и соответствующие активы, хранящиеся в среде облачных вычислений. В записях инвентаризации должно быть указано, где хранятся активы, например идентификация облачных служб	Инвентаризация активов поставщика облачных служб должна четко определять следующее: - данные потребителей облачных служб; - данные, полученные из облачных служб

Дополнительная информация для облачных служб

Существуют приложения облачных служб, которые предоставляют функции управления информацией путем добавления данных, полученных из облачных служб, к данным потребителей облачных служб. Идентификация данных, полученных из облачных служб, в качестве активов и их соответствующий учет могут способствовать повышению ИБ.

8.1.2 Владение активами

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 8.1.2.

Дополнительная информация для облачных служб

Право собственности на активы, скорее всего, будет варьироваться в зависимости от категории используемой облачной службы. При использовании службы PaaS или IaaS прикладное программное обеспечение будет принадлежать потребителю облачных служб, а при использовании службы SaaS — поставщику облачных служб.

8.1.3 Допустимое использование активов

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 8.1.3.

8.1.4 Возврат активов

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 8.1.4.

8.2 Категорирование информации

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 8.2).

8.2.1 Категорирование информации

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 8.2.1.

8.2.2 Маркировка информации

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 8.2.2. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен маркировать информацию и соответствующие активы, хранящиеся в среде облачных вычислений, в соответствии с принятыми им процедурами маркировки. В применимых случаях возможно использование функциональных возможностей маркировки, предоставляемых поставщиком облачных служб	Поставщик облачных служб должен документально оформлять и раскрывать информацию о предоставляемой им функциональности, позволяющей потребителям облачных служб классифицировать и маркировать свою информацию и соответствующие активы

8.2.3 Обращение с активами

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 8.2.3.

8.3 Обращение с носителями информации

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 8.3).

8.3.1 Управление сменными носителями информации

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 8.3.1.

8.3.2 Утилизация носителей информации

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 8.3.2.

8.3.3 Перемещение физических носителей

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 8.3.3.

9 Управление доступом

9.1 Требования бизнеса по управлению доступом

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 9.1).

9.1.1 Политика управления доступом

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002 (раздел 11).

9.1.2 Доступ к сетям и сетевым сервисам

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 9.1.2. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Политика потребителя облачных служб в отношении контроля доступа для использования сетевых служб должна определять требования к доступу пользователей по каждой отдельной используемой облачной службе	(Дополнительные рекомендации по реализации не применяются)

9.2 Процесс управления доступом пользователей

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 9.2).

9.2.1 Регистрация и отмена регистрации пользователей

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 9.2.1. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
(Дополнительные рекомендации по реализации не применяются)	Для управления доступом пользователей со стороны потребителя облачных служб поставщик облачных служб должен предоставить потребителю функции регистрации и снятия с учета пользователей, а также спецификации для использования этих функций

9.2.2 Предоставление пользователю права доступа

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 9.2.2. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
(Дополнительные рекомендации по реализации не применяются)	Поставщик облачных служб должен предоставить функции управления правами доступа пользователю облачных служб со стороны потребителя служб, а также спецификации для использования этих функций

Дополнительная информация для облачных служб

Поставщик облачных служб должен обеспечить поддержку сторонних технологий идентификации и управления доступом для своих облачных служб и соответствующих интерфейсов администрирования. Эти технологии позволяют упростить интеграцию и администрирование удостоверений пользователей между системами потребителя облачной службы и облачной службой, а также упростить использование нескольких облачных служб за счет поддержки таких возможностей, как единый вход.

9.2.3 Управление привилегированными правами доступа

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 9.2.3. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен использовать достаточные методы аутентификации (например, многофакторную аутентификацию) для аутентификации своих администраторов облачных служб при использовании возможностей администрирования облачной службы в соответствии с выявленными рисками	Поставщик облачных служб должен предоставить достаточные методы аутентификации для аутентификации администраторов облачных служб со стороны потребителя при использовании возможностей администрирования облачных служб в соответствии с выявленными рисками. Например, поставщик облачных служб может предоставить возможности многофакторной аутентификации или разрешить использование сторонних механизмов многофакторной аутентификации

9.2.4 Процесс управления секретной аутентификационной информацией пользователей

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 9.2.4. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен убедиться, что процедура управления, применяемая поставщиком службы для выделения секретной аутентификационной информации, такой как пароли, соответствует требованиям потребителя облачных служб	Поставщик облачных служб должен предоставить информацию о процедурах, которые он предоставляет для управления секретной аутентификационной информацией потребителя службы, в том числе о процедуре выделения такой информации и аутентификации пользователей

Дополнительная информация для облачных служб

Потребитель облачных служб должен контролировать управление секретной аутентификационной информацией, используя собственные или сторонние технологии идентификации и управления доступом.

9.2.5 Пересмотр прав доступа пользователей

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 9.2.5.

9.2.6 Аннулирование или корректировка прав доступа

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 9.2.6.

9.3 Ответственность пользователей

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 9.3).

9.3.1 Использование секретной аутентификационной информации

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 9.3.1.

9.4 Управление доступом к системам и приложениям

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 9.4).

9.4.1 Ограничение доступа к информации

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 9.4.1. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен обеспечить, чтобы доступ к информации облачной службы мог быть ограничен в соответствии с его политикой контроля доступа, а также чтобы такие ограничения были реализованы. Эти ограничения включают в себя ограничение доступа к облачным службам, функциям этих служб и данным потребителя облачных служб, которые хранятся в службе	Поставщик облачных служб должен предоставить средства контроля доступа, позволяющие потребителю служб ограничивать доступ к своим облачным службам, функциям служб и своим данным, которые хранятся в службе

Дополнительная информация для облачных служб

Специфика среды облачных вычислений требует дополнительного управления доступом в некоторых областях. Например, в рамках облачных служб или функций службы в таком дополнительном управлении доступом могут нуждаться функции управления гипервизором и административные консоли.

9.4.2 Безопасные процедуры входа в систему

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 9.4.2.

9.4.3 Система управления паролями

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 9.4.3.

9.4.4 Использование привилегированных служебных программ

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 9.4.4. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Если использование утилит разрешено, потребитель облачных служб должен определить утилиты, которые будут использоваться в его среде облачных вычислений, и обеспечить, чтобы они не препятствовали работе средств управления облачной службы	Поставщик облачных служб должен определить требования к утилитам, используемым в рамках облачных служб. Поставщик облачных служб должен обеспечить, чтобы утилиты, способные обойти стандартные эксплуатационные процедуры или процедуры безопасности, использовались только уполномоченным на то персоналом, и чтобы использование таких программ регулярно проверялось

9.4.5 Управление доступом к исходному коду программы

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 9.4.5.

10 Криптография

10.1 Средства криптографической защиты информации[1)]

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 10.1).

10.1.1 Политика использования средств криптографической защиты информации

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 10.1.1. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен реализовать криптографические средства защиты информации для использования облачных служб, если это оправдано проведенным анализом рисков. Эти меры должны быть достаточно эффективными для устранения выявленных рисков, независимо от того, предоставляются ли эти меры и средства потребителем или поставщиком облачных служб. Если поставщик облачных служб предлагает криптографические средства защиты информации, потребитель облачных служб должен проанализировать информацию, предоставленную поставщиком, чтобы убедиться, что эти меры: - соответствуют требованиям политики потребителя облачных служб; - совместимы с другими криптографическими средствами защиты информации, используемыми потребителем облачных служб; - применимы к данным в состоянии покоя и при передаче в облачную службу, из нее и в рамках нее	Поставщик облачных служб должен предоставить потребителю этих служб информацию об обстоятельствах, при которых он использует криптографические средства защиты обрабатываемой им информации. Поставщик облачных служб также должен предоставить потребителю служб информацию о предоставляемых им возможностях, которые могут помочь потребителю облачных служб в применении собственных криптографических средств защиты информации

Дополнительная информация для облачных служб

В некоторых юрисдикциях применение криптографических средств защиты информации может быть обязательным для определенных видов информации, таких как медицинские данные, регистрационные номера резидентов, номера паспортов и водительских прав.

10.1.2 Управление ключами

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 10.1.2. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен определить криптографические ключи для каждой облачной службы и реализовать процедуры управления ими. Если облачная служба предоставляет функции управления ключами для использования потребителем, то потребитель должен запросить следующую информацию о процедурах, используемых для управления ключами, связанными с этой службой: - типы ключей; - спецификации системы управления ключами, включая процедуры на каждом этапе жизненного цикла ключа, т. е. генерирование, изменение или обновление, хранение, удаление, извлечение, сохранение и уничтожение; - рекомендуемые процедуры управления ключами для использования потребителем облачных служб. Если потребитель облачной службы использует собственную систему управления ключами или отдельную службу управления ключами, то потребитель облачной службы не должен давать поставщику этой службы разрешение на хранение ключей шифрования для криптографических операций и управление ими	(Дополнительные рекомендации по реализации не применяются)

[1)] Применение средств криптографической защиты информации осуществляется в соответствии с законодательством Российской Федерации.

11 Физическая безопасность и защита от воздействия окружающей среды

11.1 Зоны безопасности

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 11.1).

11.1.1 Физический периметр безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 11.1.1.

11.1.2 Меры и средства контроля и управления физическим доступом

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 11.1.2.

11.1.3 Безопасность зданий, помещений и оборудования

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 11.1.3.

11.1.4 Защита от внешних угроз и угроз со стороны окружающей среды

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 11.1.4.

11.1.5 Работа в зонах безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 11.1.5.

11.1.6 Зоны погрузки и разгрузки

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 11.1.6.

11.2 Оборудование

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 11.2).

11.2.1 Размещение и защита оборудования

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 11.2.1.

11.2.2 Вспомогательные услуги

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 11.2.2.

11.2.3 Безопасность кабельной сети

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 11.2.3.

11.2.4 Техническое обслуживание оборудования

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 11.2.4.

11.2.5 Перемещение активов

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 11.2.5.

11.2.6 Безопасность оборудования и активов вне помещений организации

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 11.2.6.

11.2.7 Безопасная утилизация или повторное использование оборудования

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 11.2.7. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен запрашивать подтверждение наличия у поставщика облачных служб политик и процедур в отношении безопасной утилизации и повторного использования ресурсов	Поставщик облачных служб должен обеспечить своевременные меры для безопасной утилизации или повторного использования ресурсов (например, оборудования, хранилища данных, файлов, памяти)

Дополнительная информация для облачных служб

Дополнительная информация о безопасной утилизации содержится в ИСО/МЭК 27040.

11.2.8 Оборудование, оставленное пользователем без присмотра

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 11.2.8.

11.2.9 Политика «чистого стола» и «чистого экрана»

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 11.2.9.

12 Безопасность при эксплуатации

12.1 Эксплуатационные процедуры и обязанности

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 12.1).

12.1.1 Документально оформленные эксплуатационные процедуры

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 12.1.1.

12.1.2 Процесс управления изменениями

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 12.1.2. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
В процессе управления изменениями потребитель облачных служб должен учитывать любые изменения, вносимые поставщиком облачных служб	Поставщик облачных служб должен предоставить потребителю облачных служб информацию об изменениях в облачных службах с возможными отрицательными последствиями. Следующая информация может помочь потребителю облачных служб определить последствия изменения для ИБ: - категории изменений; - запланированные дату и время изменений; - технические параметры изменений облачных служб и базовых систем; - уведомление о начале и завершении внесения изменений. Если поставщик облачных служб предлагает службу, зависящую от другого поставщика облачных служб, то поставщик такой службы должен уведомлять потребителя этой службы об изменениях, связанных со сторонним поставщиком этой облачной службы

Дополнительная информация для облачных служб

Список параметров, которые должны содержаться в уведомлении, может быть включен в соглашение, например основное соглашение о службе или соглашение об уровне обслуживания (SLA).

12.1.3 Управление производительностью

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 12.1.3. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен обеспечить соответствие производительности облачных служб требованиям потребителя облачных служб. Потребитель облачных служб должен отслеживать использование служб и формировать прогноз требуемой производительности для обеспечения надлежащей производительности облачных служб в течение определенного периода времени	Поставщик облачных служб должен отслеживать общий объем ресурсов с целью предотвращения инцидентов ИБ, вызванных недостатком ресурсов

Дополнительная информация для облачных служб

В облачных службах задействуются ресурсы, контролируемые поставщиком облачных служб и предоставляемые потребителю на условиях основного соглашения о службе и соответствующего соглашения об уровне обслуживания. К таким ресурсам относятся программное обеспечение, аппаратное обеспечение, хранилище данных и возможности сетевого подключения.

Гибкое, масштабируемое выделение ресурсов по запросу в рамках облачных служб, как правило, повышает производительность службы. При этом потребителю облачных служб следует знать о возможных ограничениях предоставляемых ресурсов. Примерами ограничений в отношении ресурсов могут быть количество ядер процессора для приложения, объем доступного хранилища или производительность сети.

Ограничения могут быть разными, в зависимости от конкретной облачной службы или типа абонентского обслуживания, приобретаемого потребителем облачной службы. При наличии у потребителя службы требований, превосходящих существующие ограничения, потребителю необходимо сменить облачную службу или тип абонентского обслуживания.

Для управления производительностью облачных служб их потребителю необходим доступ к соответствующей статистике использования ресурсов, например:

- статистике за определенные периоды времени;
- максимальным уровням использования ресурсов.

12.1.4 Разделение сред разработки, тестирования и эксплуатации

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 12.1.4.

12.2 Защита от вредоносных программ

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 12.2).

12.2.1 Меры обеспечения информационной безопасности в отношении вредоносных программ

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 12.2.1.

12.3 Резервное копирование

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 12.3).

12.3.1 Резервное копирование информации

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 12.3.1. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
В случае предоставления поставщиком облачных служб возможностей резервного копирования потребителю облачных служб необходимо запрашивать спецификации таких возможностей у поставщика. Необходимо также проверить соответствие таких спецификаций требованиям к резервному копированию. Потребитель облачных служб несет ответственность за реализацию функций резервного копирования в тех случаях, когда поставщик облачных служб такие функции не предлагает.	Поставщик облачных служб должен предоставить спецификации своих возможностей резервного копирования потребителю облачных служб. В зависимости от ситуации, в спецификациях должна отражаться следующая информация: - объем и расписание резервного копирования; - методы резервного копирования и форматы данных, в том числе шифрование (если используется); - периоды хранения данных резервного копирования; - процедуры подтверждения целостности данных резервного копирования; - процедуры и временные рамки восстановления данных, сохраненных с помощью резервного копирования; - процедуры тестирования функций резервного копирования; - места хранения данных резервного копирования. Поставщик облачных служб должен обеспечить безопасный раздельный доступ к данным резервного копирования, таким как виртуальные снимки данных, если такая услуга предлагается потребителям облачных служб

Дополнительная информация для облачных служб

Разделение обязанностей по созданию резервных копий в среде облачных вычислений не всегда бывает четким. При предоставлении инфраструктуры как услуги (IaaS) обязанности по созданию резервных копий обычно выполняет потребитель облачных служб. Однако потребитель облачных служб может не знать о своей обязанности делать резервные копии всех своих данных, создаваемых в облачной вычислительной системе, в частности исполняемых файлов, создаваемых при применении средств для разработки платформы как услуги (PaaS).

Примечание — В качестве дополнительной услуги и за отдельную плату могут предлагаться разные уровни резервного копирования и восстановления.

В этом случае у потребителей облачных служб появляется выбор в отношении содержимого и времени резервного копирования.

12.4 Регистрация и мониторинг

Применяется цель, указанная в ИСО/МЭК 27002 (подраздел 12.4).

12.4.1 Регистрация событий

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 12.4.1. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребителю облачных служб необходимо определить требования к ведению журналов событий безопасности и проверить выполнение этих требований поставщиком служб	Поставщик облачных служб должен обеспечить возможности ведения журналов для потребителя облачных служб

Дополнительная информация для облачных служб

Обязанности потребителя и поставщика облачных служб в отношении регистрации событий варьируются в зависимости от типа используемой службы. Например, при использовании инфраструктуры как услуги (IaaS) обязанности поставщика облачных служб в отношении регистрации событий могут быть ограничены компонентами облачной инфраструктуры, а в обязанности потребителя может входить регистрация событий в своих виртуальных машинах и приложениях.

12.4.2 Защита информации регистрационных журналов

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 12.4.2.

12.4.3 Регистрационные журналы действий администратора и оператора

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 12.4.3. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Если привилегированные операции передаются в ведение потребителя облачных служб, необходимо ведение журналов действий и производительности таких операций. Потребитель облачных служб должен оценить адекватность функций ведения журналов, предлагаемых поставщиком облачных служб, и при необходимости расширить соответствующий функционал	(Дополнительные рекомендации по реализации не применяются)

Дополнительная информация для облачных служб

Процесс разделения обязанностей между потребителем и поставщиком служб облачных приложений (пункт 6.1.1) должен учитывать привилегированные операции, связанные с облачными службами. Для содействия мерам по предотвращению и исправлению неправильного использования привилегированных операций необходимы мониторинг и ведение журналов таких действий.

12.4.4 Синхронизация часов

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 12.4.4. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребителю облачных служб необходимо запросить информацию о генераторе тактового сигнала, используемом в системах поставщика облачных служб	Поставщик облачных служб должен предоставить потребителю информацию о генераторе тактового сигнала, используемом в системах поставщика облачных служб, а также информацию о том, как потребитель облачных служб может синхронизировать локальные генераторы тактового сигнала с облачным генератором тактового сигнала

Дополнительная информация для облачных служб

При использовании облачных служб необходимо обеспечить синхронизацию систем потребителя с системами поставщика облачных служб, которые обеспечивают работу служб, используемых потребителем. Отсутствие такой синхронизации может затруднять согласование событий в системах потребителя с событиями в системах поставщика облачных служб.

12.5 Контроль программного обеспечения, находящегося в эксплуатации

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 12.5).

12.5.1 Установка программного обеспечения в эксплуатируемых системах

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 12.5.1.

12.6 Менеджмент технических уязвимостей

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 12.6).

12.6.1 Процесс управления техническими уязвимостями

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 12.6.1. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель должен запросить у поставщика облачных служб информацию об управлении техническими уязвимостями, которые могут повлиять на предоставляемые облачные службы. Потребители облачных служб должны определить свою зону ответственности за технические уязвимости и выработать процессы для управления ими	Поставщик облачных служб должен предоставить потребителю облачных служб информацию об управлении техническими уязвимостями, которые могут повлиять на предоставляемые службы

12.6.2 Ограничения на установку программного обеспечения

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 12.6.2.

12.7 Особенности аудита информационных систем

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 12.7).

12.7.1 Меры обеспечения информационной безопасности в отношении аудита информационных систем

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 12.7.1.

13 Безопасность коммуникаций

13.1 Менеджмент информационной безопасности сетей

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 13.1).

13.1.1 Меры обеспечения информационной безопасности сетей

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 13.1.1.

13.1.2 Безопасность сетевых сервисов

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 13.1.2.

13.1.3 Разделение в сетях

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 13.1.3. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен определить требования к разделению сетей для изоляции пользователей в среде общего пользования службы и проверить выполнение этих требований поставщиком облачных служб	Поставщик облачных служб должен обеспечить разделение сетевого доступа в следующих случаях: - разделение пользователей в совместно арендуемых средах; - отделение внутренней административной среды поставщика облачных служб от среды облачных вычислений потребителя. В зависимости от ситуации поставщик облачных служб должен оказать содействие потребителю в проверке реализованных поставщиком мер по разделению сетей

Дополнительная информация для облачных служб

Законодательство и нормативно-правовые акты могут требовать разделения сетей или изоляции сетевого трафика.

13.2 Передача информации

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 13.2).

13.2.1 Политики и процедуры передачи информации

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 13.2.1.

13.2.2 Соглашения о передаче информации

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 13.2.2.

13.2.3 Электронный обмен сообщениями

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 13.2.3.

13.2.4 Соглашение о конфиденциальности или неразглашении

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 13.2.4.

14 Приобретение, разработка и поддержка систем

14.1 Требования к безопасности информационных систем

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 14.1).

14.1.1 Анализ и спецификации требований информационной безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 14.1.1. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен определить собственные требования ИБ к облачным службам и оценить степень соответствия этим требованиям предлагаемых поставщиком услуг. Для проведения оценки потребитель облачных служб запрашивает информацию о возможностях обеспечения ИБ у поставщика этих служб	Поставщик облачных служб предоставляет потребителям данные о мерах обеспечения ИБ, применяемых к используемым ими службам. Эти данные должны быть достаточно информативными, но при этом не должны давать злоумышленникам возможность использовать их в своих целях

Дополнительная информация для облачных служб

Необходимо ограничивать разглашение данных о реализации мер обеспечения ИБ при использовании облачных служб, предоставляемых тем потребителям или потенциальным потребителям облачных служб, с которыми заключены соответствующие соглашения о неразглашении информации.

14.1.2 Обеспечение безопасности прикладных сервисов, предоставляемых с использованием сетей общего пользования

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 14.1.2.

14.1.3 Защита транзакций прикладных сервисов

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 14.1.3.

14.2 Безопасность в процессах разработки и поддержки

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 14.2).

14.2.1 Политика безопасной разработки

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 14.2.1. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб запрашивает у их поставщика информацию об использовании поставщиком процедур и методов безопасной разработки	Поставщик облачных служб должен предоставить информацию об использовании у себя процедур и методов безопасной разработки в той степени, в которой это соответствует его собственной политике неразглашения информации

Дополнительная информация для облачных служб

Процедуры и методы безопасной разработки поставщика облачных служб могут иметь критически важное значение при использовании модели «программное обеспечение как услуга» (SaaS).

14.2.2 Процедуры управления изменениями системы

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 14.2.2.

14.2.3 Техническая экспертиза приложений (прикладных программ) после изменений операционной платформы

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 14.2.3.

14.2.4 Ограничения на изменения пакетов программ

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 14.2.4.

14.2.5 Принципы безопасного проектирования систем

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 14.2.5.

14.2.6 Безопасная среда разработки

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 14.2.6.

14.2.7 Разработка с использованием аутсорсинга

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 14.2.7.

14.2.8 Тестирование безопасности систем

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 14.2.8.

14.2.9 Приемо-сдаточные испытания системы

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 14.2.9.

Дополнительная информация для облачных служб

В сфере облачных вычислений рекомендации по приемочному испытанию системы относятся к облачным службам, которые используются потребителем этих служб.

14.3 Тестовые данные

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 14.3).

14.3.1 Защита тестовых данных

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 14.3.1.

15 Взаимоотношения с поставщиками

15.1 Информационная безопасность во взаимоотношениях с поставщиками

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 15.1).

15.1.1 Политика информационной безопасности во взаимоотношениях с поставщиками

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 15.1.1. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен отразить поставщика в своей политике ИБ во взаимоотношениях с поставщиками. Это поможет снизить риски, связанные с доступом поставщика облачных служб к данным их потребителя и управлением такими данными	(Дополнительные рекомендации по реализации не применяются)

15.1.2 Рассмотрение вопросов безопасности в соглашениях с поставщиками

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 15.1.2. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен утвердить роли и обязанности в области ИБ в связи с облачными службами согласно условиям соглашения о службе. Речь может идти о следующих процессах: - защита от вредоносного программного обеспечения; - резервное копирование; - криптографические средства защиты информации; - управление уязвимостями; - управление инцидентами; - проверка технического соответствия; - тестирование безопасности; - аудит; - сбор, хранение и защита свидетельств, в том числе журналов и документов аудита; - защита информации после прекращения действия соглашения об обслуживании; - аутентификация и контроль доступа; - идентификация и управление доступом	В рамках соглашения поставщик облачных служб должен указать меры обеспечения ИБ, направленные на устранение возможных недоразумений между поставщиком и потребителем облачных служб. Реализуемые поставщиком облачных служб меры обеспечения ИБ могут варьироваться в зависимости от типа службы, используемой потребителем

15.1.3 Цепочка поставок информационно-телекоммуникационных технологий

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 15.1.3. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
(Дополнительные рекомендации по реализации не применяются)	Если поставщик облачных служб использует облачные службы других поставщиков, от него требуется реализация мер обеспечения ИБ, которые по меньшей мере соответствуют уровню ИБ потребителей этих облачных служб. Если поставщик предоставляет облачные службы на базе цепочки поставок, такой поставщик должен обозначить задачи в области ИБ для своих поставщиков и требовать от каждого из них выполнения мероприятий по управлению рисками для осуществления этих задач

15.2 Управление услугами, предоставляемыми поставщиком

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 15.2).

15.2.1 Мониторинг и анализ услуг поставщика

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 15.2.1.

15.2.2 Управление изменениями услуг поставщика

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 15.2.2.

16 Менеджмент инцидентов информационной безопасности

16.1 Менеджмент инцидентов информационной безопасности и улучшений

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 16.1).

16.1.1 Обязанности и процедуры

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 16.1.1. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен проверить разделение обязанностей и процедур по управлению инцидентами ИБ, убедиться в их соответствии собственным требованиям	В рамках спецификаций обслуживания поставщик облачных служб должен обеспечить разделение обязанностей и процедур по управлению инцидентами ИБ между потребителем и поставщиком облачных служб. Поставщик облачных служб должен предоставить потребителю документы со следующей информацией: - перечнем инцидентов ИБ, о которых поставщик облачных служб должен сообщать своему потребителю; - описанием степени раскрытия выявленных инцидентов ИБ и соответствующих мер реагирования; - сроком направления уведомлений о выявленных инцидентах ИБ; - процедурой уведомления об инцидентах ИБ; - контактными данными ответственных за решение вопросов, связанных с инцидентами ИБ; - мерами разрешения возникающих инцидентов ИБ

16.1.2 Сообщения о событиях информационной безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 16.1.2. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб запрашивает у своего поставщика информацию о выполнении следующих процедур: - сообщения потребителя облачных служб о выявленных событиях ИБ, направляемые поставщику облачных служб; - сообщения поставщика облачных служб о выявленных событиях ИБ, направляемые потребителю облачных служб; - отслеживание потребителем облачных служб статуса сообщенного события ИБ	Поставщик облачных служб должен обеспечить выполнение следующих процедур: - сообщения потребителя облачных служб о событиях ИБ, направляемые поставщику облачных служб; - сообщения поставщика облачных служб о событиях ИБ, направляемые потребителю облачных служб; - отслеживание потребителем облачных служб статуса сообщенного события ИБ

Дополнительная информация для облачных служб

Эти процедуры должны быть дополнены необходимой информацией, например номерами телефонов, адресами электронной почты и часами работы как потребителя, так и поставщика облачных служб.

События ИБ могут выявляться как потребителем, так и поставщиком облачных служб. Поэтому главная дополнительная обязанность каждой стороны в отношении облачных служб заключается в наличии процедуры незамедлительного сообщения другой стороне о выявленном событии.

16.1.3 Сообщения о недостатках информационной безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 16.1.3.

16.1.4 Оценка и принятие решений в отношении событий информационной безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 16.1.4.

16.1.5 Реагирование на инциденты информационной безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 16.1.5.

16.1.6 Извлечение уроков из инцидентов информационной безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 16.1.6.

16.1.7 Сбор свидетельств

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 16.1.7. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель и поставщик облачных служб должны согласовать процедуры реагирования на запросы о возможном наличии цифровых свидетельств или иной информации в среде облачных вычислений.	

17 Аспекты информационной безопасности в рамках менеджмента непрерывности деятельности организации

17.1 Непрерывность информационной безопасности

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 17.1).

17.1.1 Планирование непрерывности информационной безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 17.1.1.

17.1.2 Реализация непрерывности информационной безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 17.1.2.

17.1.3 Проверка, анализ и оценивание непрерывности информационной безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 17.1.3.

17.2 Резервирование оборудования

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 17.2).

17.2.1 Доступность средств обработки информации

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 17.2.1.

18 Соответствие

18.1 Соответствие правовым и договорным требованиям

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 18.1).

18.1.1 Идентификация применимых законодательных и договорных требований

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 18.1.1. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен проанализировать возможность применимости законодательства и нормативно-правовых актов юрисдикций поставщика таких служб, помимо законодательства и правовых актов, непосредственно регулирующих деятельность потребителя облачных служб. Потребитель облачных служб запрашивает свидетельства выполнения своим поставщиком важных для потребителя требований соответствующих нормативно-правовых актов и стандартов. В качестве таких свидетельств могут служить сертификаты сторонних проверяющих организаций	Поставщик облачных служб должен информировать своего потребителя о требованиях правовой юрисдикции, регулирующих их предоставление. Поставщик облачных служб должен быть осведомлен о действующих в его отношении законодательных требованиях (например, о шифровании для защиты персональных данных). Эта информация должна предоставляться по запросу потребителя облачных служб. Поставщик облачных служб должен предоставить своему потребителю свидетельства выполнения требований действующего законодательства и договорных обязательств

Дополнительная информация для облачных служб

Необходима осведомленность о законодательных и нормативных требованиях, действующих в отношении использования облачных служб, особенно в тех случаях, когда функции обработки, хранения и передачи данных географически распределены по нескольким юрисдикциям.

Следует отметить, что ответственность за соблюдение требований (как правовых, так и договорных) по-прежнему лежит на потребителе облачных услуг и не может быть переложена на поставщика облачных услуг.

18.1.2 Права на интеллектуальную собственность

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 18.1.2. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Установка лицензионного коммерческого программного обеспечения в облачной службе может приводить к нарушению условий лицензий. Потребитель облачных служб должен предусмотреть процедуру выяснения лицензионных требований в отношении облачных служб перед выдачей разрешения на установку лицензионного программного обеспечения в облачной среде. Особого внимания требуют гибкие и масштабируемые облачные среды, где программное обеспечение может использоваться на большем количестве систем или ядер процессоров, чем допускают условия лицензий	Поставщик облачных служб должен внедрить процесс реагирования на жалобы, касающиеся нарушений прав интеллектуальной собственности

18.1.3 Защита записей

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 18.1.3. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб запрашивает у своего поставщика информацию о защите собираемых и хранимых им записей об использовании облачных служб потребителем	Поставщик облачных служб предоставляет потребителю этих служб информацию о защите собираемых и хранимых поставщиком записей об использовании облачных служб потребителем

18.1.4 Конфиденциальность и защита персональных данных

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 18.1.4.

Дополнительная информация для облачных служб

В ИСО/МЭК 27018 содержится свод правил по защите персональных данных в публичных облаках, используемых для их обработки.

18.1.5 Регулирование криптографических мер обеспечения информационной безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 18.1.5. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен убедиться в том, что набор криптографических мер обеспечения ИБ, используемых при предоставлении облачных служб, соответствует действующим соглашениям, законодательным и нормативным требованиям	Поставщик облачных служб предоставляет своему потребителю описание реализованных им криптографических мер обеспечения ИБ для определения соответствия требованиям действующих соглашений, законодательных и нормативных актов

18.2 Проверки информационной безопасности

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 18.2).

18.2.1 Независимая проверка информационной безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 18.2.1. Применяются также следующие рекомендации, касающиеся облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб запрашивает у своего поставщика документальные свидетельства по реализации мер обеспечения ИБ облачных служб, заявляемых поставщиком служб. Среди прочего, такие свидетельства могут включать в себя сертификаты соответствия действующим стандартам	Поставщик облачных служб должен предоставить потребителю этих служб документальные свидетельства реализации заявленных им мер обеспечения ИБ. В тех случаях, когда проведение отдельного аудита потребителем облачных служб не представляется целесообразным или может повысить риск ИБ, поставщик облачных служб должен обеспечить независимые свидетельства реализации мер обеспечения ИБ в соответствии с политиками и процедурами поставщика облачных служб. Эти свидетельства должны предоставляться потенциальным потребителям облачных служб до заключения договора. В качестве независимого аудита должен использоваться приемлемый на усмотрение поставщика облачных служб метод оценки его операций с учетом интересов потребителей и при условии обеспечения достаточной прозрачности. В тех случаях, когда проведение независимого аудита представляется нецелесообразным, поставщик облачных служб должен провести проверку своих собственных операций, обеспечив прозрачность ее процедуры и результатов для потребителей облачных служб

18.2.2 Соответствие политикам и стандартам безопасности

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 18.2.2. Применяются также следующие рекомендации, касающиеся облачных служб.

18.2.3 Анализ технического соответствия

Применяются меры обеспечения ИБ, соответствующие им рекомендации по реализации и дополнительная информация, определенные в ИСО/МЭК 27002, пункт 18.2.3.

Приложение А
(обязательное)

Расширенный набор мер обеспечения информационной безопасности для облачных служб

Это приложение является неотъемлемой частью настоящего стандарта.

В настоящем приложении содержится описание дополнительных мер обеспечения ИБ, а также рекомендации по их реализации, представляющие собой расширенный набор мер обеспечения ИБ для облачных служб. Представленные в настоящем приложении меры обеспечения ИБ не дублируют меры обеспечения ИБ, приведенные в ИСО/МЭК 27002.

Организации, желающие реализовать эти меры в СМИБ, отвечающей требованиям ИСО/МЭК 27001, должны включить в Положение о применимости (Statement of Applicability, SOA) меры обеспечения ИБ, указанные в настоящем приложении.

CLD.6.3 Взаимоотношения между потребителями и поставщиками облачных служб

Цель: разъяснение порядка взаимоотношений между потребителем и поставщиком облачных служб в контексте общих ролей и обязанностей с целью обеспечения ИБ.

CLD.6.3.1 Общие роли и обязанности в среде облачных вычислений

Мера обеспечения ИБ

Необходимо разделение обязанностей между определенными сторонами в контексте общих ролей по обеспечению ИБ. Обязанности должны быть задокументированы, доведены до сведения потребителя и поставщика облачных служб и выполнены ими.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен определить или дополнить свои существующие политики и процедуры в соответствии со спецификой использования облачных служб, а также должен информировать пользователей облачных служб о своих ролях и обязанностях при использовании этих служб	Поставщик облачных служб должен задокументировать и сообщить о своих возможностях, ролях и обязанностях в области ИБ при использовании своих облачных служб, а также о ролях и обязанностях в сфере безопасности, которые потребитель облачных служб должен реализовать и контролировать в рамках собственного использования служб

Дополнительная информация для облачных служб

В сфере облачных вычислений роли и обязанности, как правило, разделены между сотрудниками потребителя и сотрудниками поставщика облачных служб. При разделении ролей и обязанностей следует принимать во внимание данные и приложения потребителя облачных служб, хранителем которых является поставщик облачных служб.

CLD.8.1 Ответственность за активы

Применяется цель, определенная в ИСО/МЭК 27002 (подраздел 8.1).

CLD.8.1.5 Удаление активов клиента облачных служб

Мера обеспечения ИБ

Активы потребителя облачных служб, хранимые в помещениях поставщика таких служб, должны своевременно удаляться и при необходимости должны быть возвращены после прекращения действия соглашения об облачной службе.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб запрашивает документальное описание процесса прекращения обслуживания, включая процедуру возвращения и удаления облачных активов потребителя, в том числе удаления всех копий этих активов из систем поставщика облачных служб. Описание процесса прекращения обслуживания должно содержать список всех активов вместе с графиком прекращения обслуживания в установленные сроки	Поставщик облачных служб должен предоставить информацию о мерах, предпринятых для возвращения и удаления всех активов потребителя облачных служб после прекращения действия соглашения об их использовании. Порядок возврата и удаления активов отражается в соглашении и осуществляется в установленные сроки. В описании процесса прекращения обслуживания должны быть указаны все возвращаемые и удаляемые активы

CLD.9.5 Контроль доступа к данным потребителя облачных служб в виртуальной среде совместного использования

Цель: снижение рисков ИБ в совместно используемой виртуальной среде облачных вычислений.

CLD.9.5.1 Разделение в виртуальных вычислительных средах

Мера обеспечения ИБ

Виртуальная среда потребителя облачных служб, работающая в облачной среде, должна быть защищена от доступа со стороны других потребителей облачных служб и прочих пользователей, не имеющих соответствующих разрешений.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
(Дополнительные рекомендации по реализации не применяются)	Поставщик облачных служб должен обеспечить надлежащее логическое разделение данных потребителей облачных служб, виртуализированных приложений, операционных систем, хранилищ и сетей для решения следующих задач: - разделения ресурсов, используемых потребителями облачных служб в совместно арендуемых средах; - отделения внутренней административной инфраструктуры поставщика служб от ресурсов, используемых потребителями облачных служб. В совместно арендуемых облачных службах поставщик должен внедрить меры обеспечения ИБ для надлежащей изоляции ресурсов, используемых различными арендаторами. Поставщик облачных служб должен учитывать риски, связанные с запуском программного обеспечения, предоставляемого клиентом в рамках служб, предлагаемых поставщиком облачных служб

Дополнительная информация для облачных служб

Реализация логического разделения зависит от технологий, применяемых для виртуализации:

- конфигурации сети и хранилища могут виртуализироваться в тех случаях, когда функция виртуализации ПО обеспечивает виртуальную среду (например, виртуальную операционную систему). Кроме этого, разделение потребителей облачных служб в средах с программной виртуализацией может быть спроектировано и реализовано с помощью программных функций;

- если информация потребителей облачных служб хранится в местах с общим физическим доступом и таблицей метаданных облачных служб, то изоляция информации от других потребителей облачных служб может быть реализована путем контроля доступа через таблицу метаданных.

Описание безопасной работы в совместно арендуемых средах с соответствующими инструкциями, которое содержится в ИСО/МЭК 27040, может применяться к облачным службам.

CLD.9.5.2 Защита виртуальных машин

Мера обеспечения ИБ

Чтобы удовлетворить потребности бизнеса, необходимо обеспечить защиту виртуальных машин в среде облачных вычислений.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
При настройке виртуальных машин потребители и поставщики облачных служб должны обеспечить защиту соответствующих аспектов (например, только тех портов, протоколов и служб, которые необходимы) и наличие соответствующих технических мер (например, средства противодействия вредоносному ПО, ведение журналов регистрации) для каждой используемой виртуальной машины	

CLD.12.1 Эксплуатационные процедуры и обязанности

Применяется цель, указанная в ИСО/МЭК 27002 (подраздел. 12.1).

CLD.12.1.5 Безопасность операций администратора

Мера обеспечения ИБ

Необходимо определить, задокументировать и проверить процедуры, применяемые к административным операциям в облачных службах.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб должен отразить в документации процедуры для критически важных операций, сбой которых может нанести непоправимый ущерб облачной вычислительной среде. Примеры критически важных операций: - установка, модификация и удаление виртуализированных устройств, таких как серверы, сети и хранилища; - процедуры прекращения предоставления облачных служб; - резервное копирование и восстановление. В документе должно быть указано на необходимость контроля над этими операциями со стороны отдельного сотрудника	Поставщик облачных служб должен предоставить документацию о критически важных операциях и процедурах потребителям облачных служб, при необходимости

Дополнительная информация для облачных служб

Преимуществом облачных вычислений является возможность быстрого обеспечения обслуживания и его администрирования, а также возможность предоставления услуг самообслуживания по запросу. Эти операции зачастую выполняются администраторами потребителя и поставщика облачных служб. Поскольку постороннее вмешательство в эти операции может приводить к серьезным инцидентам ИБ, необходимо рассмотреть процедуры защиты таких операций, а также разработать и реализовать эти процедуры при необходимости. Среди примеров таких серьезных инцидентов можно указать стирание или остановку работы большого количества виртуальных серверов или уничтожение виртуальных активов.

CLD.12.4 Регистрация и мониторинг

Применяется цель, указанная в ИСО/МЭК 27002 (подраздел 12.4).

CLD.12.4.5 Мониторинг облачных служб

Мера обеспечения ИБ

У потребителя облачных служб должна быть возможность отслеживать определенные аспекты работы используемых им облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
Потребитель облачных служб запрашивает у поставщика информацию о возможностях мониторинга обслуживания, поддерживаемых каждой облачной службой	Поставщик облачных служб должен обеспечить потребителю возможность мониторинга определенных аспектов работы служб, используемых потребителем. Например, возможность отслеживания использования облачной службы в качестве платформы для злонамеренных атак или утечек конфиденциальных данных из облачной службы. Использование функций мониторинга должно быть защищено средствами управления доступом. Эти средства должны обеспечивать доступ только к той информации, которая относится к собственным экземплярам облачных служб их потребителя. Поставщик облачных служб должен предоставить потребителю этих служб документацию о средствах мониторинга служб. В процессе мониторинга необходимо обеспечить возможность получения данных, сопоставимых с журналами событий (пункт 12.4.1) и содействующих выполнению условий соглашения об уровне обслуживания

CLD.13.1 Безопасность связи

Применяется цель, указанная в ИСО/МЭК 27002 (подраздел 13.1).

CLD.13.1.4 Согласованность методов обеспечения безопасности виртуальных и физических сетей

Мера обеспечения ИБ

После конфигурирования виртуальных сетей необходимо проверить согласованность конфигураций виртуальных и физических сетей исходя из политики сетевой безопасности поставщика облачных служб.

Рекомендации по реализации для облачных служб

Потребитель облачных служб	Поставщик облачных служб
(Дополнительные рекомендации по реализации не применяются)	Поставщик облачных служб должен разработать и отразить в документации политику ИБ в отношении настроек виртуальной сети в координации с политикой безопасности в отношении физической сети. Поставщик облачных служб должен убедиться в том, что конфигурация виртуальной сети соответствует политике ИБ, вне зависимости от средств, используемых для создания конфигурации

Дополнительная информация для облачных служб

В среде облачных вычислений, построенной по технологии виртуализации, виртуальная сеть настраивается в виртуальной инфраструктуре физической сети. Несоответствие положений сетевых политик в таких средах может приводить к перебоям в работе систем или нарушению контроля доступа.

Примечание — В зависимости от типа облачных служб, обязанности по настройке виртуальной сети могут по-разному распределяться между потребителем и поставщиком облачных служб.

Приложение В
(справочное)

Ссылки на документы, касающиеся рисков информационной безопасности, связанных с облачными вычислениями

Настоящее приложение не является неотъемлемой частью настоящего стандарта.

Надлежащее использование мер обеспечения ИБ, предусматриваемых настоящим стандартом, основано на оценке и анализе рисков ИБ организации. Несмотря на важность этих аспектов, вопросы оценки и анализа рисков ИБ не являются основным предметом настоящего стандарта. Ниже приводится список ссылок на документы, которые включают в себя описания источников рисков и самих рисков, связанных с предоставлением и использованием облачных служб. Следует отметить, что источники рисков и сами риски могут варьироваться в зависимости от типа и характера службы, а также новых технологий облачных вычислений. Пользователям настоящего стандарта следует использовать актуальные версии документов по мере необходимости.

Рекомендация МСЭ-Т X.1601 «Платформа безопасности для облачных вычислений». Январь 2014 г.

Департамент управления информацией правительства Австралии. «Контрольные показатели конфиденциальности и облачных вычислений для государственных органов Австралии: практические рекомендации». Февраль 2013 г.

Центр кибербезопасности Австралии. «Безопасность облачных вычислений для арендаторов». Декабрь 2014 г. http://www.asd.gov.au/publications/protect/Cloud_Computing_ Security_for_Tenants.pdf

Центр кибербезопасности Австралии. «Безопасность облачных вычислений для поставщиков облачных служб». Декабрь 2014 г. http://www.asd.gov.au/publications/protect/ Cloud_Computing_Security_for_Cloud_Service Providers.pdf

OGCIO, Гонконг. «Контрольный список по обеспечению конфиденциальности обработки персональных данных поставщиками облачных служб в облачных платформах». Апрель 2013 г.

OGCIO, Гонконг. «Контрольный список по безопасности для потребителей облачных служб». Январь 2013 г.

Национальный институт стандартов и технологий. SP800-144 «Рекомендации по обеспечению конфиденциальности в публичных облачных вычислениях». Декабрь 2011 г.

Национальный институт стандартов и технологий. SP800-146 «Краткий обзор облачных вычислений с рекомендациями». Май 2012 г.

SPRING Singapore. Приложение А «Оценка рисков для безопасности при виртуализации, сингапурский технический справочник 30:2012. Технический справочник по безопасной виртуализации серверов». Март 2012 г.

SPRING Singapore. Приложение А «Контрольный список по безопасности и аспекты уровня обслуживания при проверке платформы SaaS, сингапурский технический справочник 31:2012. Технический справочник по безопасности и рекомендации в отношении уровня обслуживания при использовании публичных облачных служб». Март 2012 г.

SPRING Singapore. Приложение А «Раскрытие информации поставщиками облачных служб, сингапурский стандарт SS584:2013. Спецификация многоуровневой безопасности облачных вычислений». Август 2013 г.

SPRING Singapore. Приложение В «Контрольный список по безопасности и аспекты уровня обслуживания при проверке платформы IaaS, сингапурский технический справочник 31:2012. Технический справочник по безопасности и рекомендации в отношении уровня обслуживания при использовании публичных облачных служб». Март 2012 г.

SPRING Singapore, сингапурский стандарт SS584:2013 «Спецификация многоуровневой безопасности облачных вычислений». Август 2013 г.

SPRING Singapore, сингапурский технический справочник 30:2012 «Технический справочник по безопасности виртуализации серверов». Март 2012 г.

SPRING Singapore, сингапурский технический справочник 31:2012 «Технический справочник по безопасности и рекомендации в отношении уровня обслуживания при использовании публичных облачных служб». Март 2012 г.

Федеральная программа управления рисками и авторизацией США (FedRAMP PMO) «Базовые контрольные меры по безопасности FedRAMP», версия 2.0. Июнь 2014 г.

Cloud Security Alliance «Матрица средств управления облачной среды». Сентябрь 2013 г.

ENISA «Оценка рисков безопасности облачных вычислений». Ноябрь 2009 г.

ENISA «Базовая система контроля информации в облачных вычислениях». Ноябрь 2009 г.

ISACA «Вопросы безопасности в облачных вычислениях». Июль 2011 г.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным и межгосударственным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального и межгосударственного стандарта
ISO/IEC 17788	IDT	ГОСТ ISO/IEC 17788—2016 «Информационные технологии. Облачные вычисления. Общие положения и терминология»
ISO/IEC 17789	—	*
ISO/IEC 27000	—	*
ISO/IEC 27002—2013	—	*

* Соответствующий национальный стандарт отсутствует. До его принятия рекомендуется использовать перевод на русский язык данного международного стандарта. Официальный перевод данного международного стандарта находится в Федеральном информационном фонде стандартов.

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

- IDT — идентичный стандарт.

Библиография

Recommendation ITU-T X.805 (2003) Security architecture for systems providing end-to-end communications

ISO/IEC 17203:2011 Information technology — Open Virtualization Format (OVF) specification

ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements

ISO/IEC 27005:2011 Information technology — Security techniques — Information security risk management

ISO/IEC 27018:2014 Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC 27036-1:2014 Information technology — Security techniques — Information security for supplier relationships — Part 1: Overview and concepts

ISO/IEC 27036-2:2014 Information technology — Security techniques — Information security for supplier relationships — Part 2: Requirements

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

ISO/IEC CD 27036-4 Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services — (Under development)

ISO/IEC 27040:2015 Information technology — Security techniques — Storage security

ISO 19440:2007 Enterprise integration — Constructs for enterprise modelling

ISO 31000:2009 Risk management — Principles and guidelines

NIST, SP 800-145 2011 The NIST Definition of Cloud Computing

NIST 2009 Effectively and Securely Using the Cloud Computing Paradigm

ENISA 2009 Cloud Computing Benefits, risks and recommendations for information security

Cloud Security Alliance, Security Guidance for Critical Areas of Focus in Cloud Computing V3.0

Cloud Security Alliance, Top Threats to Cloud Computing V1.0

Cloud Security Alliance, Domain 12: Guidance for Identity & Access Management V2.1

ISACA, Cloud Computing: Business Benefits With Security, Governance and Assurance Perspectives

ISACA, Cloud Computing Management Audit/Assurance Program

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

Ключевые слова: облачные вычисления, поставщик облачных служб, потребитель облачных служб, меры обеспечения ИБ

Технический редактор *В.Н. Прусакова*
Корректор *О.В. Лазарева*
Компьютерная верстка *Л.А. Круговой*

Сдано в набор 21.05.2021. Подписано в печать 28.05.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 4,65. Уч.-изд. л. 4,30.

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