ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО 24143— 2025

Информация и документация

СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ ИНФОРМАЦИЕЙ

Концепция и принципы

(ISO 24143:2022, IDT)

Издание официальное

Москва
Российский институт стандартизации
2025

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным бюджетным учреждением «Российский институт стандартизации» (ФГБУ «Институт стандартизации») и Обществом с ограниченной ответственностью «ЭОС Тех» (ООО «ЭОС Тех») на основе собственного перевода на русский язык англоязычной версии стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 459 «Информационная поддержка жизненного цикла изделий»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 25 июня 2025 г. № 620-ст

4 Настоящий стандарт идентичен международному стандарту ИСО 24143:2022 «Информация и документация. Стратегическое управление информацией. Концепция и принципы» (ISO 24143:2022 «Information and documentation — Information Governance — Concept and principles», IDT)

5 ВВЕДЕН ВПЕРВЫЕ

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

© ISO, 2022
© Оформление. ФГБУ «Институт стандартизации», 2025

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

Содержание

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 1
4 Преимущества стратегического управления информацией 3
5 Принципы стратегического управления информацией 4
Приложение А (справочное) Диаграммы взаимосвязи понятий 8
Библиография 10

Введение

Информация — это критически значимый актив, необходимый для поддержки деловых процессов и являющийся основой эффективности любой профессиональной деятельности. Вследствие многочисленных существующих и появляющихся форм и вариантов использования информации, а также связанных с ее применением в организациях, как правило, возникают определенные трудности, связанные с внедрением согласованных систем хранения, поиска, извлечения, распространения и анализа поступающей информации. Глобальная цифровая трансформация и изменения в общественных ожиданиях должны сопровождаться большей прозрачностью, подотчетностью, защитой персональных данных, безопасностью, интероперабельностью и обменом информацией как внутри организаций, так и между ними. Эта тенденция подразумевает обоснование взвешенного подхода с целью стратегического управления информацией и направлена на поддержку деловых процессов на надлежащем уровне и инициатив в области цифровой трансформации. Большинство государственных и неправительственных органов и организаций во всем мире учитывают преимущества координации на стратегическом уровне целого ряда дисциплин, связанных с информацией, данными и знаниями.

Настоящий стандарт определяет понятия и принципы стратегического управления информацией.

В настоящем стандарте рассмотрены руководящие принципы стратегического управления с целью продуктивного, соответствующего нормативно-правовым требованиям, безопасного, прозрачного и подотчетного создания, использования, обеспечения долговременной сохранности и уничтожения/передачи на архивное хранение информации, которую могут применять владельцы, члены совета директоров, партнеры, представители высшего руководства организаций и т. д.

Стратегическое управление информацией, будучи неотъемлемой частью общего управления организацией, определяет общие высокоуровневые принципы, способствующие эффективному и продуктивному сотрудничеству всех специалистов информационного профиля для поддержки и достижения долгосрочных целей организации. В такого рода сотрудничество могут быть вовлечены представители следующих направлений деятельности (перечень не является исчерпывающим):

- управление данными;
- управление информацией;
- управление документами;
- управление знаниями;
- обеспечение исполнения нормативно-правовых и иных установленных требований;
- электронная сохранность (обеспечение долговременной сохранности электронных документов и информации);
- информационная безопасность;
- корпоративная архитектура;
- защита персональных данных;
- открытые данные;
- большие данные;
- искусственный интеллект (ИИ);
- блокчейн и распределенные реестры;
- управление деловыми процессами;
- менеджмент качества.

Стратегическое управление информацией требует согласованности и интеграции с соответствующими стандартами систем менеджмента, такими как стандарты серий ИСО 9000, ИСО 27000 и ИСО 30300.

Стратегическое управление информацией — это стратегическая рамочная концепция управления информационными активами в масштабе всей организации с целью достижения ожидаемых результатов ее деятельности и обеспечения потенциальных результатов относительно того, что риски для использования определенной информации и, следовательно, для ведения оперативной деятельности, а также для целостности организации надлежащим образом выявляются и регулируются. Стратегическое управление информацией включает в себя (не ограничиваясь) политики, процессы, процедуры, роли и меры контроля и управления, реализованные с целью исполнения нормативно-правовых требований управления рисками и удовлетворения потребностей хозяйственной деятельности.

Стратегическое управление информацией представляет собой всеобъемлющую высокоуровневую концепцию, которая:

- обеспечивает согласованность всей связанной с информацией деятельности с миссией и целями организации, а также с ее деловыми, правовыми и общественными обязательствами;
- обеспечивает всесторонний систематический подход к информации посредством интеграции процессов, имеющих отношение к управлению и контролю над информацией;
- поддерживает сотрудничество между заинтересованными сторонами;
- создает высокоуровневую основу для управления информацией вне зависимости от ее формы, типа и формата; оказывает влияние на программы образования и повышения квалификации персонала и на осведомленность о связанных с информацией обязательствах, рисках и возможностях.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информация и документация

СТРАТЕГИЧЕСКОЕ УПРАВЛЕНИЕ ИНФОРМАЦИЕЙ

Концепция и принципы

Information and documentation.
Information Governance.
Concept and principles

Дата введения — 2026—06—01

1 Область применения

Настоящий стандарт определяет понятия и принципы стратегического управления информацией.

Настоящий стандарт предназначен для применения в целях стратегического управления унаследованными, текущими и планируемыми информационными активами организации. Он может быть использован в организациях разного масштаба и представлен в любых секторах, включая государственные и частные компании, государственные учреждения и некоммерческие организации.

2 Нормативные ссылки

В настоящем стандарте нормативные ссылки отсутствуют.

3 Термины и определения

В настоящем стандарте применены следующие термины с соответствующими определениями.

ИСО и МЭК ведут терминологические базы данных для использования в стандартизации по следующим адресам:

- Электропедия МЭК, доступная по адресу: gost.e-ecolog.ru ;
- платформа онлайн-просмотра ИСО, доступная по адресу: gost.e-ecolog.ru .

3.1 Термины, относящиеся к информации

3.1.1 **аутентичный, аутентичность** (authentic, authenticity): Свойство, которым информация (3.1.3) обладает, если может быть доказано, что она является именно тем, чем претендует быть.

Примечание 1 — Свойство аутентичности подразумевает, что информация создана или отправлена именно тем действующим лицом, которое в ней указано в качестве создателя или отправителя, и что она создана или отправлена именно в то время, которое в ней указано.

Примечание 2 — Когда можно доказать, что информация является именно тем, чем она претендует быть, ее можно называть аутентичной информацией.

Примечание 3 — См. рисунок А.1.

[ИСО 30300:2020, 3.2.2, модифицированное — термин «документы» (records) заменен термином «информация». Термин «аутентичный» (authentic) заменен на термин «аутентичность» (authenticity). Добавлено новое примечание 2]

Издание официальное

3.1.2 **данные** (data): Набор букв или символов, которым придан или может быть придан определенный смысл.

Примечание 1 — См. рисунок А.1.

[ИСО 30300:2020, 3.2.4]

3.1.3 **информация** (information): Данные (3.1.2), имеющие конкретный смысл в определенном контексте.

Примечание 1 — См. рисунок А.1.

[ИСО 30300:2020, 3.2.7]

3.1.4 **информационный актив** (information asset): Информация (3.1.3), имеющая ценность для заинтересованной стороны.

Примечание 1 — См. рисунок А.1.

[ISO/TS 17573-2:2020, 3.95, модифицированное — термин «информация» использован вместо фразы «знания и данные»]

3.1.5 **целостность** (integrity): Свойство информации, являющейся полной и неизмененной.

Примечание 1 — См. рисунок А.1.

[ИСО 30300:2020, 3.2.8, модифицированное — термин «документы» заменен на термин «информация»]

3.2 Термины, относящиеся к стратегическому управлению информацией

3.2.1 **соответствие** (compliance): Характеристика, отражающая соблюдение правил, установленных законом, нормативным актом, стандартом или политикой.

Примечание 1 — См. рисунок А.2.

[ИСО/МЭК 20924:2021, 3.1.10, модифицированное — в определение добавлено слово «характеристика». Добавлено примечание]

3.2.2 **электронная непрерывность**, **цифровая непрерывность** (digital continuity): Способность использовать электронную (цифровую) информацию (3.1.3) надлежащим образом и по мере необходимости.

Примечание 1 — См. рисунок А.2.

3.2.3 **уничтожение/передача информации** (disposition): Совокупность процессов, связанных с выполнением решений, касающихся хранения информации (3.1.3) в течение установленных сроков и ее последующего уничтожения либо передачи.

Примечание 1 — См. рисунок А.2.

[ИСО 30300:2020, 3.4.8, модифицированное — термин «документы» заменен термином «информация», текст определения сокращен с сохранением смысла]

3.2.4 **электронное раскрытие;** *e*-раскрытие (electronic discovery; e-discovery): Процесс выявления, сбора, обеспечения сохранности, анализа и представления сохраняемой в электронном виде информации с целью ее использования в качестве электронных (цифровых) доказательств.

Примечание 1 — В английском языке наряду с термином «e-discovery» также используются термины «ediscovery», «eDiscovery», «e-Discovery», «E-discovery», «electronic discovery».

Примечание 2 — К сохраняемой в электронном виде информации (electronically stored information, ESI), в частности, относят электронные форматы, электронную почту, документы, презентации, базы данных, сообщения голосовой почты, аудио- и видеофайлы.

Примечание 3 — Электронное раскрытие, как правило, воспринимается как форма цифрового расследования, когда во исполнение полученного в ходе судебного процесса или расследования запроса о предоставлении доказательств проводят поиск таких доказательств среди сохраняемой электронным образом информации.

Примечание 4 — См. рисунок А.2.

3.2.5 **структура, концептуальная структура, концепция** (framework): Структура, состоящая из взаимосвязанных частей и предназначенная для поддержки выполнения конкретной задачи.

Примечание 1 — См. рисунок А.2.

[ИСО 15638-6:2014, 4.30]

3.2.6 **стратегическое управление** (governance): Принципы, политики и концепции, посредством которых направляется, контролируется и управляется деятельность организации.

Примечание 1 — См. рисунок А.2.

[ISO/IEEE 11073-10201:2020, 3.1.25, модифицированное — фраза «процессы и спецификации» заменена на фразу «состоящая из взаимосвязанных частей»]

3.2.7 **стратегическое управление информацией** (information governance): Стратегическая определенная концепция управления информационными активами (3.1.4) в масштабе всей организации с целью достижения предпочтительных результатов ее деятельности и уверенности в том, что риски, связанные с владением информацией (3.1.3) и, следовательно, с возможностью ведения безопасной оперативной деятельности, а также с целостностью (3.1.5) организации, эффективно выявляются и управляются.

Примечание 1 — Стратегическое управление информацией включает в себя (не ограничиваясь ими) политики, процессы, процедуры, роли и меры контроля и управления, реализованные с целью исполнения нормативно-правовых требований, управления рисками и удовлетворения потребностей оперативной деятельности.

Примечание 2 — Данные являются одной из форм информационного актива.

Примечание 3 — См. рисунок А.2.

3.2.8 **информационная безопасность** (information security): Сохранение конфиденциальности, целостности и доступности информации (3.1.3).

Примечание 1 — См. рисунок А.2.

[ИСО/МЭК 27000:2018, 2.28]

4 Преимущества стратегического управления информацией

4.1 Общие положения

Стратегическое управление информацией представляет собой стратегическую, междисциплинарную рамочную концепцию, поддерживающую сотрудничество между специалистами тех профессий, которые по роду деятельности связаны с управлением информацией. Данная концепция, в которой информация рассмотрена как ценный корпоративный актив, потенциально может обеспечить перечисленные ниже преимущества.

4.2 Стратегические преимущества

Стратегическое управление информацией:

a) предполагает внедрение всесторонней высокоуровневой концепции стратегического управления, которая направлена на реализацию миссии организации и позволяет получить экономические и стратегические преференции, включая следующие:

1) максимизация деловой отдачи, получаемой от использования информационных активов,
2) защита прав организации и других заинтересованных сторон,
3) исполнение нормативно-правовых требований, а также
4) повышение открытости, прозрачности и подотчетности;

b) поддерживает принятие обоснованных решений посредством обеспечения своевременного доступа к аутентичной, надежной, релевантной, полной и точной, актуальной и доступной информации;

c) снижает риски, способные привести к репутационному ущербу, финансовым потерям или штрафам, посредством:

1) принятия адекватных мер обеспечения безопасности и защиты ценных информационных активов,
2) уничтожения или очистки информации, которую более не требуется сохранять;

d) выявляет пробелы в системах, политиках, процедурах и процессах, необходимых для эффективного управления информационными активами организации;

e) поддерживает согласованность политик организации и их гармонизированное применение в плане безопасности информации и защиты персональных данных, проведения экспертизы ценности, обеспечения сохранности, уничтожения либо передачи, а также поиска и раскрытия информации;

f) обеспечивает механизм для включения всех информационных активов в программу стратегического управления;

g) устраняет разобщенность и разногласия между представителями различных профессий и способствует совместному междисциплинарному подходу при внедрении инновационных технологий, согласованному со стратегическими целями и приоритетами организации;

h) поддерживает этичное стратегическое управление в отношении инновационных технологий, таких как искусственный интеллект и блокчейн.

4.3 Преимущества в оперативной деятельности

Стратегическое управление информацией:

a) обеспечивает всесторонний систематический подход к управлению информацией, посредством которой поддерживается оперативная деятельность организации, интеграция таких связанных с управлением и контролем над информацией направлений деятельности, как управление информацией, информационная безопасность, защита персональных данных, обеспечение исполнения нормативно-правовых требований, непрерывного процесса деловой деятельности и восстановление после катастроф, электронное раскрытие и др.;

b) устанавливает объем и характер информации в организации, ее местонахождение, какие действия в отношении данной информации можно предпринять и как следует управлять и контролировать ее, выявляет наиболее ценную информацию, которую можно многократно использовать;

c) поддерживает систематическую организацию информационных активов, обеспечивая более высокий уровень доступности, информационного обмена и сотрудничества, а также более быстрый поиск и оперативное извлечение деловой информации;

d) обеспечивает концептуальную основу для поддержания и хранения информационных активов, направленную на предотвращение утраты критически значимой деловой информации;

e) снижает затраты на хранение и расходование ресурсов, необходимых для управления или выявления информации посредством реализации программы ее уничтожения/передачи, в рамках которой уничтожается та информация, которая более не актуальна и/или которую более не требуется сохранять;

f) снижает затраты на предоставление информации в ходе *e*-раскрытия, а также обеспечивает отсутствие появления у организации дополнительных рисков вследствие создания и сохранения бóльших объемов информации, чем это необходимо;

g) способствует сохранению корпоративной культуры и памяти, формируя основу для расширения возможностей по обеспечению электронной (цифровой) непрерывности, коллективно достигаемой на уровне предприятия.

5 Принципы стратегического управления информацией

5.1 Признание информации стратегическим корпоративным активом

В стратегическом управлении информацией такой ресурс, как информация организации, рассматривают как актив (согласно определению в 3.2.8). Информация имеет стратегическое значение для развития любой организации и способствует ее жизнеспособности в долговременной перспективе.

Стратегическое управление информацией учитывает юридическую, деловую, историческую и иную ценность информации и информационных активов, их важнейшую роль в деловой деятельности и в стратегическом управлении, связанные с информацией преимущества и риски, а также потенциал информационных активов в плане ключевого конкурентного преимущества.

Стратегическое управление информацией охватывает структурированную и неструктурированную, нецифровую и цифровую информацию, а также интеллектуальную информацию.

5.2 Проектирование стратегического управления информацией в качестве ключевого элемента корпоративной стратегии

Стратегическое управление информацией включает в себя все высокоуровневые, стратегические аспекты управления информацией и контроля, такие как: обеспечение инфраструктуры и систем для обработки информации; исполнение касающихся информации нормативно-правовых требований; ин-

струменты стратегического управления, например политики, процедуры и стандарты, а также людские ресурсы (подбор кадров, их обучение и повышение квалификации).

5.3 Интеграция стратегического управления информацией в структуры стратегического управления организацией

Стратегическое управление информацией должно являться частью общего стратегического корпоративного управления — системы, посредством которой осуществляются направление деятельности организации и контроль над ней (см. ИСО/МЭК 38500) для достижения целей организации и для удовлетворения этических требований в отношении ее целостности, традиций и социальной ответственности сотрудников.

Стратегическое управление информацией является неотъемлемой частью всех структур стратегического управления и систем оперативного управления организации. Стратегическое управление информацией интегрируется со всеми структурами и системами управления информацией, такими как процессы управления финансами, рисками, безопасностью, качеством, окружающей средой, здоровьем работников и безопасностью труда, и с их оперативными требованиями и процедурами. Стратегическое управление информацией должно находить отражение в сводной отчетности организации.

Стратегическое управление информацией должно охватывать все информационно-ориентированные аспекты и области стратегического управления, включая в том числе управление документами, защиту персональных данных, информационную безопасность, управление грифами доступа, управление данными, управление корпоративным контентом, контроль исполнения и *e*-раскрытие.

5.4 Обеспечение лидерства и поддержки со стороны высшего руководства

Высшее руководство должно принять на себя ответственность за руководство, лидерство и обеспечение поддержки стратегического управления информацией. Должен быть назначен представитель высшего руководства организации, который будет персонально отвечать за стратегическое управление информацией и обеспечивать подотчетность, докладывая о текущем положении дел первому лицу организации либо высшей структуре стратегического управления организации.

В обязанности данного представителя, отвечающего за стратегическое управление информацией в организации, должно входить установление компонентов концепции организации стратегического управления информацией, определение процессов, процедур и управление ими, устранение потенциальных и реальных препятствий, информирование о целях и деловых задачах, выделение необходимых ресурсов (кадры, структуры, инфраструктуры) и информирование высшего руководства о ходе работы.

Ответственный за стратегическое управление информацией контролирует всю эту деятельность в рамках последовательной программы стратегического управления информацией.

Кроме того, ответственность за оперативные аспекты стратегического управления информацией может быть делегирована уполномоченному сотруднику по стратегическому управлению информацией и/или другим сотрудникам соответствующего уровня.

5.5 Реализация стратегического управления информацией на основе кооперации и сотрудничества

Стратегическое управление информацией понимается прежде всего как стратегическая междисциплинарная концепция, которая формирует основу для сотрудничества и синергии между представителями разных профессий, имеющими отношение к использованию информации.

Общей целью такого сотрудничества является всестороннее согласованное стратегическое и оперативное управление различными информационными активами в масштабе всей организации.

Конкретными аспектами принципа реализации стратегического управления информацией на основе кооперации и сотрудничества являются:

- инклюзивность — вовлечение всех заинтересованных сторон;
- всесторонность — охват всех информационных активов, как существующих, так и потенциальных;
- последовательность политики — отсутствие слабых звеньев в сохранении и защите ключевых знаний, информации и данных с целью достижения целей по безопасности, защите персональных данных и по исполнению нормативно-правовых требований;
- гибкость — активное взаимодействие в инициативном порядке с инновационными информационными дисциплинами и заинтересованными сторонами;

- сотрудничество — поощрение и поддержка междисциплинарных усилий, а также принятие решений на основе консенсуса; в пересекающихся областях должно отдаваться предпочтение коллективным усилиям вместо установления жестких междисциплинарных границ.

5.6 Обеспечение поддержки в рамках стратегического управления информацией исполнения нормативно-правовых требований и выполнения иных обязательных требований

В рамках стратегического управления информацией осуществляют поддержку и исполнение всех действующих законов и нормативных актов, обязательных стандартов и стандартов добровольного применения, кодексов отраслевой практики, применимых к оперативной деятельности организации.

5.7 Согласованность стратегического управления информацией с целями деловой деятельности

Стратегическое управление информацией должно быть согласовано со стратегическими и оперативными целями и задачами организации и потребностями деловой деятельности, что следует постоянно контролировать и пересматривать по мере текущих изменений в деятельности организации.

При разработке программы стратегического управления информацией следует учитывать все требования и запросы заинтересованных сторон.

5.8 Обеспечение поддержки в рамках стратегического управления информацией информационной безопасности и защиты персональных данных

Стратегическое управление информацией должно содействовать информационной безопасности и защите персональных данных, в том числе поддержку. Управление доступом и разрешения на доступ к наиболее значимой информации должны быть установлены и реализованы таким образом, чтобы обеспечить доступность информации только тем, кто обладает соответствующими полномочиями.

5.9 Обеспечение поддержки в рамках стратегического управления информацией качества и целостности информации

Стратегическое управление информацией должно способствовать тому, чтобы обеспечить следующие характеристики информации:

- аутентичность;
- достоверность информации;
- полнота и согласованность информационных данных (обеспечиваемые в масштабе всей организации);
- надежность;
- релевантность;
- простота извлечения и использования;
- точность;
- доказуемая целостность.

5.10 Содействие развитию культуры сотрудничества и обмену знаниями

Эффективное и продуктивное стратегическое управление информацией, как правило, подразумевает отношение к информации как к корпоративному ресурсу, а не как к активу, контролируемому исключительно какой-либо конкретной службой, или подразделением, или отдельным лицом.

В рамках стратегического управления информацией, где это необходимо и уместно, должно быть осуществлено сотрудничество между различными службами и подразделениями с целью максимизации деловой отдачи от информации.

Обмен информацией и ее коллективное использование следует осуществлять таким образом, чтобы информация находилась в постоянном доступе (в т. ч. повторно), чтобы можно было доставлять и обмениваться ею. Рекомендуется обеспечивать доступ к информации по нескольким каналам, при этом неизменно следует соблюдать требования конфиденциальности, защиты персональных данных и безопасности.

Информационные системы (как цифровые, так и не цифровые) и процессы следует проектировать таким образом, чтобы обеспечивать интероперабельность, поддерживая тем самым сотрудничество и обмен знаниями.

5.11 Внедрение подходов на основе менеджмента риска

В стратегическом управлении информацией следует внедрять подход на основе анализа рисков и реализовывать средства контроля над надлежащим использованием информации в соответствии с требованиями законов, нормативных актов и политик, учитывая профиль/степень риска организации.

5.12 Обеспечение наличия и доступности информации для авторизованных заинтересованных сторон

Стратегическое управление информацией должно содействовать эффективности оперативной деятельности организации и обеспечивать доступность релевантной информации авторизованным пользователям/потребителям в требуемое время, в требуемом месте и в требуемом формате с учетом экономически рациональных затрат.

Стратегическое управление информацией должно поддерживать конкурентоспособность и жизнестойкость организации.

Программа стратегического управления информацией должна постоянно адаптироваться с тем, чтобы удовлетворять возрастающим внутренним потребностям как организации, так и внешних сторон.

5.13 Стратегическое управление информацией на протяжении всего ее жизненного цикла

Информацией следует управлять на протяжении всего ее жизненного цикла, от момента создания или получения (а иногда от разработки политик и процедур, проектирования информационных систем) и вплоть до окончательного уничтожения и даже после него (например, некоторые метаданные могут быть сохранены с целью исполнения нормативно-правовых требований).

5.14 Поддержка корпоративной культуры

Стратегическое управление информацией должно стать неотъемлемой частью культуры организации, а также поведения и взаимоотношения сотрудников организации.

Влияние стратегического управления информацией на поведение сотрудников организации зависит от их лидерских качеств на всех уровнях и от четко сформулированных ценностей организации, а также от признания значимости стратегического управления информацией и реализации мер по его продвижению. При отсутствии соответствующих интеграционных процессов на всех уровнях организации существует риск негативных последствий.

Применение стратегического управления информацией требует планового подхода к реализации и управлению ее изменениями, обеспечивающего возможность проявления осведомленности в этой области сотрудникам и, как следствие, исполнения ими всех требований при использовании программ организации по стратегическому управлению информацией.

5.15 Поддержка устойчивого развития

Стратегическое управление информацией является частью социально ответственного поведения организаций и способствует их устойчивому развитию.

Приложение А
(справочное)

Диаграммы взаимосвязи понятий

А.1 Поддержка корпоративной культуры

Понятия между собой взаимосвязаны. Анализ взаимосвязей между понятиями в области стратегического управления информацией и формирование на этой основе системы понятий являются предпосылкой для создания словаря.

Такой анализ проведен при разработке словаря терминов, определенных в настоящем стандарте. В данном приложении приведены диаграммы взаимосвязей между понятиями для иллюстрации подобного рода процессов.

В данном приложении использованы три вида связей (отношений) между понятиями в соответствии с ИСО 704:

a) ассоциативные отношения (показаны двусторонними стрелками). Ассоциативные отношения не являются иерархическими и имеют место в том случае, когда между понятиями на основании опыта может быть установлена тематическая связь (см. ИСО 704:2009, 5.5.3);

b) партитивные отношения (показаны линиями без стрелок). Партитивные отношения являются иерархическими. Считается, что партитивное (разделительное) отношение имеет место тогда, когда суперординатное понятие представляет собой целое, а субординатные понятия — это части этого целого. Части совместно образуют целое (см. ИСО 704:2009, 5.5.2.3.1);

c) родовые отношения (показаны линиями без стрелок). Родовые отношения являются иерархическими. Родовое отношение существует между двумя понятиями, когда сущность подчиненного понятия включает сущность главного понятия плюс по крайней мере одну дополнительную разграничивающую характеристику (см. ИСО 704:2009, 5.5.2.2.1).

А.2 Диаграммы взаимосвязи понятий

А.2.1 Общие положения

На рисунках А.1 и А.2 показаны диаграммы взаимосвязи понятий. Диаграммы выделяют тематические группы основных понятий, связанные с условиями и концепциями стратегического управления информацией.

Так как термины приведены без определений и связанных с ними примечаний, более подробная информация приведена в разделе 3.

А.2.2 Понятия, относящиеся к информации

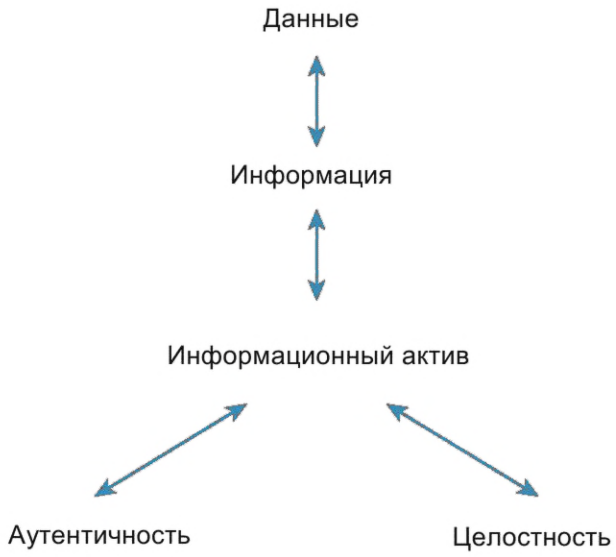

Рисунок А.1 — Основные понятия, относящиеся к информации

А.2.3 Понятия, относящиеся к стратегическому управлению информацией

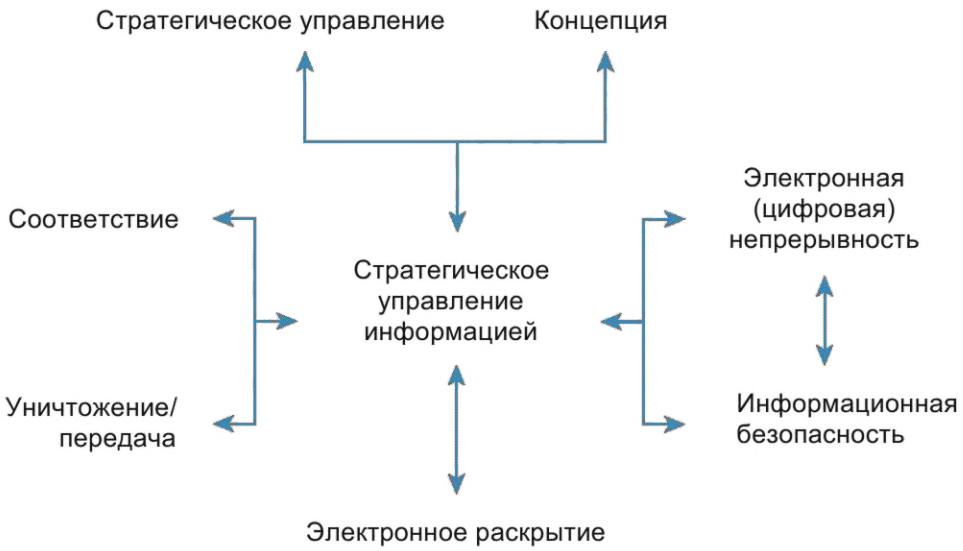

Рисунок А.2 — Основные понятия, относящиеся к информации

Библиография

[1] ISO 704:2022, Terminology work — Principles and methods (Терминологическая работа. Принципы и методы)

[2] ISO/IEC TR 10032:2003, Information technology — Reference Model of Data Management (Информационные технологии. Справочная модель управления данными)

[3] ISO/IEEE 11073-10201:2020, Health informatics — Device interoperability — Part 10201: Point-of-care medical device communication — Domain information model (Информатизация здоровья. Обмен данными с персональными медицинскими приборами. Часть 10201. Информационная модель предметной области)

[4] ISO/TR 14639-2:2014, Health informatics — Capacity-based eHealth architecture roadmap — Part 2: Architectural components and maturity model (Информатика в здравоохранении. Архитектурная дорожная карта электронного здравоохранения на базе возможностей. Часть 2. Компоненты архитектуры и модель завершенности)

[5] ISO 15489-1:2016, Information and documentation — Records management — Part 1: Concepts and principles (Информация и документация. Управление документами. Часть 1. Понятия и принципы)

[6] ISO 15638-6:2014, Intelligent transport systems — Framework for collaborative Telematics Applications for Regulated commercial freight Vehicles (TARV) — Part 6: Regulated applications [Интеллектуальные транспортные системы. Структура совместных телематических приложений для регулируемых коммерческих грузовых транспортных средств (TARV). Часть 6. Регулируемые приложения]

[7] ISO/IEC 15944-8:2012, Information technology — Business operational view — Part 8: Identification of privacy protection requirements as external constraints on business transactions (Информационная технология. Бизнес-операционное представление. Часть 8. Идентификация требований защиты конфиденциальности как внешние ограничения на деловые операции)

[8] ISO 16439:2014, Information and documentation — Methods and procedures for assessing the impact of libraries (Информатика и документация. Методы и процедуры оценки влияния библиотек)

[9] ISO/TS 17187:2019, Intelligent transport systems — Electronic information exchange to facilitate the movement of freight and its intermodal transfer — Governance rules to sustain electronic information exchange methods (Интеллектуальные транспортные системы. Электронный обмен информацией для ускорения перевозки грузов и их перегрузки на все виды транспорта. Руководящие правила по обеспечению электронных методов обмена информацией)

[10] ISO/TS 17573-2:2020, Electronic fee collection — System architecture for vehicle related tolling — Part 2: Vocabulary (Электронный сбор платежей. Архитектура систем для взимания платы за проезд транспортных средств. Часть 2. Словарь)

[11] ISO/TR 18128:2014, Information and documentation — Risk assessment for records processes and systems (Информация и документация. Оценка рисков для документных процессов и систем)

[12] ISO/TR 19591:2018, Personal protective equipment for firefighters — Standard terms and definitions (Средства индивидуальной защиты пожарных. Стандартные термины и определения)

[13] ISO/IEC 20924:2024, Internet of Things (IoT) and digital twin — Vocabulary [Интернет вещей (ИВ) и цифровой двойник. Словарь]

[14] ISO 21505:2017, Project, programme and portfolio management — Guidance on governance (Управление проектами, программами и портфелями. Руководство по организационному руководству)

[15] ISO/TR 21965:2019, Information and documentation — Records management in enterprise architecture (Информация и документация. Управление записями в корпоративной архитектуре)

[16] ISO 22316:2017, Security and resilience — Organizational resilience — Principles and attributes (Безопасность и устойчивость к негативным внешним воздействиям. Устойчивость организации. Принципы и качественные признаки)

[17] ISO 24531:2013, Intelligent transport systems — System architecture, taxonomy and terminology — Using XML in ITS standards, data registries and data dictionaries [Интеллектуальные транспортные системы (ИТС). Архитектура системы, таксономия и терминология. Применение языка XML в стандартах на ИТС, регистрах и словарях данных]

[18] ISO/IEC TR 26927:2011, Information technology — Telecommunications and information exchange between systems — Corporate telecommunication networks — Mobility for enterprise communications (Информационные технологии. Телекоммуникации и обмен информацией между сетями. Корпоративные телекоммуникационные сети. Мобильность для учрежденческой связи)

[19] ISO/IEC 27000:2018, 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)

[20] ISO/IEC 27050, Information technology — Electronic discovery [Информационные технологии. Выявление и раскрытие электронной информации (электронное раскрытие)]

[21] ISO/IEC 27014:2020, Information security, cybersecurity and privacy protection — Governance of information security (Информационные технологии. Информационная безопасность, кибербезопасность и защита конфиденциальности. Руководство деятельностью по обеспечению информационной безопасности)

[22] ISO 30300:2020, Information and documentation — Records management — Core concepts and vocabulary (Информация и документация. Системы управления документами. Основные положения и словарь)

[23] ISO 37000:2021, Governance of organizations Guidance (Управление организациями. Руководство)

[24] ISO 31000:2018, Risk management — Guidelines (Менеджмент риска. Принципы и руководство)

[25] ISO/TR 31004:2013, Risk management — Guidance for the implementation of ISO 31000 (Менеджмент риска. Руководство по внедрению ИСО 31000)

[26] ISO 37001:2016, Anti-bribery management systems — Requirements with guidance for use (Системы менеджмента борьбы со взяточничеством. Требования и руководство по применению)

[27] ISO 37002:2021, Whistleblowing management systems Guidelines (Системы управления сообщениями о фактах коррупции или незаконной деятельности. Руководящие указания)

[28] ISO 37301:2021, Compliance management systems Requirements with guidance for use [Системы комплаенс-менеджмента. Требования и руководство по применению]

[29] ISO/IEC 38500:2024, Information technology Governance of IT for the organization (Информационные технологии. Управление ИТ в организации)

[30] ISO/IEC TR 38502:2017, Information technology — Governance of IT — Framework and model (Информационная технология. Стратегическое управление ИТ. Структура и модель)

[31] ISO/IEC TR 38504:2016, Governance of information technology — Guidance for principles-based standards in the governance of information technology (Управление информационными технологиями. Руководство для стандартов на основе принципов в области управления информационными технологиями)

[32] ISO/IEC 38505-1:2017, Information technology — Governance of IT — Governance of data — Part 1: Application of ISO/IEC 38500 to the governance of data (Информационная технология. Стратегическое управление ИТ. Стратегическое управление данными. Часть 1. Применение ИСО/МЭК 38500 для менеджмента данных)

УДК 005.921.5:005.912:006.354 ОКС 01.140.20

Ключевые слова: информация, документация, стратегическое управление информацией, управлении документами, управление данными, концепция, принципы

Редактор *Л.С. Зимилова*
Технический редактор *В.Н. Прусакова*
Корректор *С.И. Фирсова*
Компьютерная верстка *М.В. Малеевой*

Сдано в набор 27.06.2025. Подписано в печать 07.07.2025. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 2,32. Уч.-изд. л. 2,12.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении в ФГБУ «Институт стандартизации»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
gost.e-ecolog.ru gost.e-ecolog.ru