**Пояснительная записка**

**к СТ РК ISO 19650-5-2020 «Организация и оцифровка информации о зданиях и работах в области гражданского строительства, включая информационное моделирование строительных объектов (BIM). Управление информацией с использованием информационного моделирования строительных объектов. Часть 5. Подход к управлению информацией, ориентированный на безопасность»**

**1 Техническое обоснование разработки стандарта**

Настоящий стандарт разрабатывается во исполнение пункта 16 Дорожной карты по цифровизации всех этапов жизненного цикла строительного объекта с применением технологии информационного моделирования строительных объектов (BIM-технологий), расширению области применения управления проектами на всех стадиях жизненного цикла строительного объекта и разработке нового СТ РК ОУП (офис управления проектами).

Цель разработки настоящего стандарта состоит в обеспечении непрерывности управления информацией на всем протяжении жизненного цикла зданий и сооружений.

**2 Основание для разработки стандарта**

Инициативная разработка

**3 Характеристика объекта стандартизации**

Настоящий стандарт распространяется на национальные стандарты по применению технологии информационного моделирования строительных объектов (building information modelling; BIM), разрабатываемые на территории Республики Казахстан.

Настоящий стандарт обеспечивает основу для оказания организациям помощи в понимании ключевых проблем уязвимости и характера средств контроля, необходимых для управления возникающими рисками безопасности.

Подход, ориентированный на безопасность, может применяться на протяжении всего жизненного цикла инициативы, проекта, актива, продукта или услуги, будь то планируемый или существующий объект, когда получена, создана, обработана и/или сохранена конфиденциальная информация, в том числе с использованием информационного моделирования строительных объектов (BIM).

Настоящий стандарт может применяться ко всем типам активов, а также всем типам и видам организаций, независимо от выбранной стратегии закупок.

**4 Сведения о взаимосвязи проекта стандарта с техническими регламентами и документами по стандартизации**

Проект стандарта реализует положения:

– Закона Республики Казахстан «Об архитектурной, градостроительной и строительной деятельности в Республике Казахстан» от 16 июля 2001 года № 242-II.

**5 Предполагаемые пользователи стандарта**

Настоящий стандарт предназначен в первую очередь для использования:

– ответственными лицами, участвующими в управлении активами и объектами;

– ответственными лицами, участвующими в определении назначений и содействии совместной работе на всем протяжении жизненного цикла актива;

– ответственными лицами, участвующими в управлении активами и объектами на этапе эксплуатации актива; и

– ответственными лицами, которые участвуют в определении информации, необходимой для целей эксплуатации, которая должна быть собрана во время поставки актива.

**6 Сведения о рассылке проекта стандарта на согласование**

Проект стандарта направлен на согласование и рассмотрение: органам государственного управления, НПП «Атамекен», техническим комитетам и другим субъектам.

**7 Информация о результатах научных исследований (испытаний) и измерений, документах по стандартизации и иных документах, на основе которых разрабатывается проект стандарта**

Проект стандарта разработан на основе международного стандарта ISO 19650–5:2021 «Организация и оцифровка информации о зданиях и работах в области гражданского строительства, включая информационное моделирование строительных объектов (BIM). Управление информацией с использованием информационного моделирования строительных объектов. Часть 5. Этап эксплуатации активов».

**8 Данные о разработчике и соисполнителях (контактные данные), сроках разработки проекта стандарта**

Разработчик – ТОО «Научно-исследовательский институт «Алматыгенплан»

Срок – декабрь 2022 года

*Проект (1 редакция)*

*Изображение государственного Герба Республики Казахстан*

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН**

**Организация и оцифровка информации о зданиях и работах в области гражданского строительства,** **включая информационное моделирование строительных объектов (BIM)**

**УПРАВЛЕНИЕ ИНФОРМАЦИЕЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННОГО МОДЕЛИРОВАНИЯ СТРОИТЕЛЬНЫХ ОБЪЕКТОВ**

**Часть 5**

**Подход к управлению информацией, ориентированный на безопасность**

**СТ РК ISO 19650-5-2020**

*(ISO 19650-5:2020 Organization and digitalization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling – Part 5: Security-minded approach to information management, IDT)*

*Настоящий проект стандарта не подлежит применению до его утверждения*

**Комитет технического регулирования и метрологии**

**Министерства торговли и интеграции Республики Казахстан (Госстандарт)**

**Нур-Султан**

**Предисловие**

**1 ПОДГОТОВЛЕН И ВНЕСЕН** ТОО «Научно-исследовательский институт «Алматыгенплан»

**2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ** Приказом Комитета технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан №\_\_\_\_\_от \_\_\_\_.

**3** Настоящий стандарт идентичен международному стандарту ISO 19650–5:2020 Organization and digitalization of information about buildings and civil engineering works, including building information modelling (BIM) — Information management using building information modelling – Part 5: Security-minded approach to information management (Организация и оцифровка информации о зданиях и работах в области гражданского строительства, включая информационное моделирование строительных объектов (BIM). Управление информацией с использованием информационного моделирования строительных объектов. Часть 5. Подход к управлению информацией, ориентированный на безопасность).

Международный стандарт подготовлен Техническим комитетом по стандартизации ISO/TC 59, Строительные объекты и строительные работы, Подкомитетом SC 13, Организация и оцифровка информации о зданиях и работах в области гражданского строительства, включая информационное моделирование строительных объектов (BIM), в сотрудничестве с Европейским комитетом по стандартизации.

Перевод с английского языка (en).

Официальные экземпляры международного стандарта, на основе которого подготовлен настоящий национальный стандарт и на который даны ссылки, имеются в Едином государственном фонде нормативных технических документов.

Официальной версией настоящего стандарта является текст на государственном и русском языках. В разделе «Нормативные ссылки» и тексте стандарта ссылочные международные стандарты актуализированы. Степень соответствия – (IDT).

**4** В настоящем стандарте реализованы нормы Законов Республики Казахстан «О стандартизации» от 5 октября 2018 года № 183-VІ, «Об архитектурной, градостроительной и строительной деятельности в Республике Казахстан» от 16 июля 2001 года № 242-II.

**5 ВВЕДЕН ВПЕРВЫЕ**

*Информация об изменениях к настоящему стандарту публикуется в ежегодно издаваемом информационном каталоге «Документы по стандартизации», а текст изменений и поправок – в периодически издаваемых информационных каталогах «Национальные стандарты». В случае пересмотра (замены) или отмены настоящего стандарта соответствующее уведомление будет опубликовано в ежемесячно издаваемом информационном каталоге «Национальные стандарты».*

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Комитета технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан.

**Содержание**

[Введение IV](#_bookmark2)

1. Область применения 1
2. Нормативные ссылки 1
3. Термины и определения 2
4. Установление необходимости подхода, ориентированного на безопасность с использованием процесса оценки конфиденциальности 4
5. Инициирование подхода, ориентированного на безопасность 8
6. Разработка стратегии безопасности 10
7. Разработка плана управления безопасностью 12
8. Разработка плана управления нарушениями безопасности/инцидентами 15
9. Работа с назначенными сторонами 17

Приложение А (*информационное*) Информация о контексте безопасности 20

Приложение B (*информационное*) Информация о типах персонала, физических и технических средствах контроля безопасности и управления информационной безопасностью 22

Приложение C (*информационное*) Оценка, касающаяся предоставления информации третьим сторонам 26

Приложение D (*информационное*) Соглашение о совместном использовании информации 28

Библиография 30

**Введение**

Построенная среда переживает период быстрой эволюции. Ожидается, что внедрение информационного моделирования строительных объектов (Building Information Modelling; BIM) и все более широкое использование цифровых технологий при проектировании, строительстве, производстве, эксплуатации и управлении активами или продуктами, а также предоставлении услуг в антропогенной среде окажут преобразующее влияние на все вовлеченные стороны. Вполне вероятно, что инициативы или проекты, в ходе которых создаются новые активы или решения, или модифицируются и управляются существующие, должны носить более совместный характер, чтобы быть более эффективными и результативными. Такое сотрудничество требует более прозрачных, открытых способов работы и, насколько это возможно, надлежащего распределения и использования цифровой информации.

Комбинирование физической и цифровой среды должно будет обеспечить достижение будущих налоговых, финансовых, функциональных целей, а также целей в области устойчивого развития и роста. Это окажет влияние на процессы закупок, поставки и эксплуатации, включая более тесное междисциплинарное и секторальное сотрудничество. Это также приведет к более широкому использованию цифровых инструментов и доступности информации. Использование компьютерных технологий уже поддерживает новые способы работы, такие как разработка за пределами строительной площадки, заводское производство и автоматизация на месте. Сложные киберфизические системы, использующие датчики (кибер- или вычислительный элемент) для управления физическими частями систем или воздействия на них, способны работать в режиме реального времени, чтобы влиять на результаты в реальном мире. Ожидается, что такие системы будут использоваться для достижения таких преимуществ, как повышение энергоэффективности и улучшение управления жизненным циклом активов за счет сбора информации в режиме реального времени об их использовании и состоянии. Их уже можно найти в транспорте, коммунальных службах, инфраструктуре, зданиях, производстве, здравоохранении и обороне, и когда они способны взаимодействовать как интегрированные киберфизические среды, их можно использовать для развития интеллектуальных сообществ.

В результате такого растущего использования информационно-коммуникационных технологий и зависимости от них возникает необходимость в решении присущих им проблем уязвимости и, следовательно, возникающих последствий для безопасности, как в отношении антропогенной среды, так и для активов, продуктов, услуг, отдельных лиц или сообществ, а также любой связанной с ними информации.

Настоящий стандарт обеспечивает основу для оказания организациям помощи в понимании ключевых проблем уязвимости и характера средств контроля, необходимых для управления возникающими рисками безопасности до уровня, приемлемого для соответствующих сторон. Его цель никоим образом не состоит в том, чтобы подорвать сотрудничество или преимущества, которые BIM, другие методы совместной работы и цифровые технологии могут генерировать.

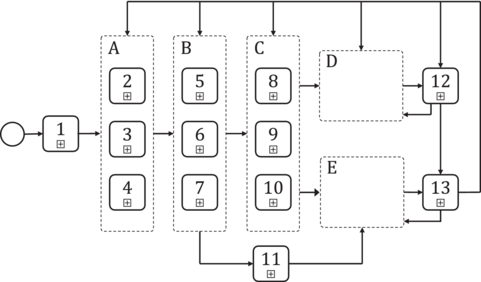
Термин «организация» охватывает не только назначающие стороны и назначенные стороны, как определено в ISO 19650–1, но и организации, которые непосредственно не участвуют в назначении.

Требования по информационной безопасности для отдельной организации, организационного подразделения или системы изложены в стандарте ISO/IEC 27001, но не могут применяться в нескольких организациях.

BIM и другие цифровые методы и технологии совместной работы, как правило, предполагают совместный обмен информацией между широким кругом независимых организаций в секторе антропогенной среды. Поэтому в настоящем стандарте рекомендуется применять подход, ориентированный на безопасность и основанный на учете рисков, который может применяться как между организациями, так и внутри них. Надлежащий и соразмерный характер подхода также проявляется в таком преимуществе, как отсутствие мер запрещающих участие малых и средних предприятий в команде поставки.

Подход, ориентированный на безопасность, может применяться на протяжении всего жизненного цикла инициативы, проекта, актива, продукта или услуги, будь то планируемый или существующий объект, когда получена, создана, обработана и/или сохранена конфиденциальная информация.

На рисунке 1 показана интеграция данного подхода, ориентированного на безопасность, с другими корпоративными стратегиями, политикой, планами и требованиями к информации для реализации проектов с поддержкой цифровых технологий, а также обслуживания и эксплуатации активов с использованием BIM.



**Условные обозначения:**

A скоординированные и согласованные стратегии и политики

B скоординированные и согласованные планы

C скоординированные и согласованные требования к информации

D деятельность, осуществляемая на этапе эксплуатации активов

E деятельность, осуществляемая на этапе поставки активов (см. также ISO 19650–2)

1 корпоративные планы и цели

2 стратегический план/политика управления активами (см. ISO 55000)

3 стратегия безопасности

4 другие корпоративные стратегии и политики

5 план управления активами (см. ISO 55000)

6 план управления безопасностью

7 другие корпоративные планы

8 требования к информации об активе (Asset Information Requirements; AIR)

9 требования по информационной безопасности (которые являются частью плана управления безопасностью)

10 корпоративные требования к информации (Organizational Information Requirements; OIR)

11 стратегический бизнес-кейс и краткое описание стратегии

12 операционное использование активов

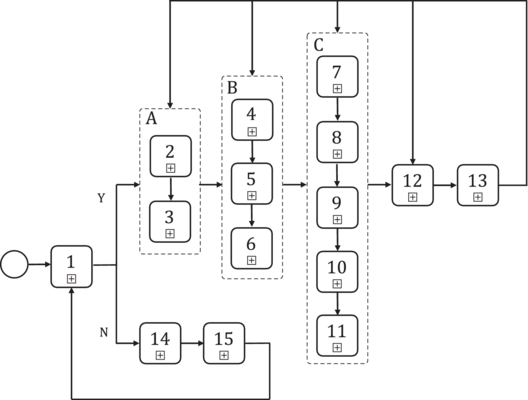
13 измерение производительности и действия по улучшению

Примечание – Нумерация в A, B и C не подразумевает никакого порядка

**Рисунок 1 – Интеграция подхода, ориентированного на безопасность, в рамках более широкого процесса BIM**

Примечание – Обратитесь к ISO 19650–1 за концепциями и принципами, включая корпоративные требования к информации (OIR) и требования к информации по активу (AIR), чтобы помочь дальнейшему пониманию безопасности в контексте серии ISO 19650.

Процесс принятия решения о необходимости и реализации (где это уместно) подхода, ориентированного на безопасность в управлении информацией представлен на рисунке 2.



**Условные обозначения:**

A инициирование подхода ориентированного на безопасность

B разработка стратегии безопасности

C разработка плана обеспечения безопасности

Y да

N нет

1 определение с использованием процесса сортировки безопасности требуется ли подход ориентированный на безопасность

2 создание механизмов управления, подотчетности и ответственности для подхода ориентированного на безопасность

3 начало разработки подхода ориентированного на безопасность

4 оценка рисков в области безопасности

5 разработка мер по снижению уровня опасности

6 допустимые риски по безопасности документов

7 разработка политик и процедур в целях осуществления мер по смягчению последствий нарушения безопасности

8 разработка требований по информационной безопасности

9 разработать требований, касающихся предоставления информации третьим лицам

10 разработка требований к материально-технической безопасности

11 разработка плана при нарушении безопасности/управление инцидентами

12 работа с назначенными сторонами в рамках официальных контрактов и вне их, при внедрении подхода, ориентированного на безопасность, включая разработку соглашений о совместном использовании информации, когда это необходимо

13 мониторинг, аудит и просмотр

14 защита любой конфиденциальной коммерческой и персональной информации (никакого другого подхода, ориентированного на безопасность, не требуется)

15 просмотр на наличие изменений в инициативе, проекте, активе, продукте или услуге, которые могут повлиять на их конфиденциальность

**Рисунок 2 – Процесс реализации подхода, ориентированного на безопасность, изложенного в данном документе**

Реализация мер, изложенных в настоящем стандарте, поможет снизить риск потери, неправильного использования или изменения конфиденциальной информации, которая может повлиять на безопасность, надежность и устойчивость активов, продуктов, окружающей среды или услуг, предоставляемых ими, из них или через них. Это также поможет защитить от потери, кражи или разглашения коммерческой информации, персональной информации и интеллектуальную собственность. Любые подобные инциденты могут привести к значительному репутационному ущербу, что отразится на упущенных выгодах и отвлечении ресурсов на проведение расследований, принятие решений и деятельность средств массовой информации, в дополнение к срыву и задержке повседневной операционной деятельности. Кроме того, в тех случаях, когда происходят инциденты, и информация становится общедоступной, практически невозможно восстановить всю эту информацию или предотвратить ее дальнейшее распространение.

**НАЦИОНАЛЬНЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН**

**Организация и оцифровка информации о зданиях и работах в области гражданского строительства, включая информационное моделирование строительных объектов (BIM)**

**УПРАВЛЕНИЕ ИНФОРМАЦИЕЙ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННОГО МОДЕЛИРОВАНИЯ СТРОИТЕЛЬНЫХ ОБЪЕКТОВ**

**Часть 5**

**Подход к управлению информацией, ориентированный на безопасность**

**Дата введения \_\_\_\_**

**1 Область применения**

Настоящий стандарт устанавливает общие понятия и принципы соответствующие стадии зрелости, называемой «информационное моделирование строительных объектов (BIM)», согласно ISO 19650, а также устанавливает управление конфиденциальной информацией, которая получена, создана, обработана и сохранена в рамках или в связи с инициативой, проектом, активом, продуктом или услугой.

В настоящем стандарте рассматриваются шаги, необходимые для создания и развития надлежащего и соразмерного мышления и культуры безопасности в организациях, имеющих доступ к конфиденциальной информации, включая необходимость мониторинга и аудита соответствия.

Описанный подход применим на протяжении всего жизненного цикла инициативы, проекта, актива, продукта или услуги, планируемых или существующих, когда получена, создана, обработана и/или сохранена конфиденциальная информация.

Настоящий стандарт предназначен для использования любой организацией, применяющей управление информацией и технологии при создании, проектировании, строительстве, производстве, эксплуатации, управлении, модификации, улучшении, сносе и/или утилизации активов или продуктов, а также предоставлении услуг в пределах антропогенной среды. Изложенная в настоящем стандарте информация также будет интересна и актуальна для тех организаций, которые хотят защитить свою коммерческую информацию, персональную информацию и интеллектуальную собственность.

Настоящий стандарт может применяться ко всем типам активов, а также ко всем типам и видам организаций, независимо от выбранной стратегии закупок.

**2 Нормативные ссылки**

Для применения настоящего стандарта необходимы следующие ссылочные документы по стандартизации:

СТ РК ISO 19650–2 Организация и оцифровка информации о зданиях и работах в области гражданского строительства, включая информационное моделирование строительных объектов (BIM). Управление информацией с использованием информационного моделирования строительных объектов. Часть 2. Этап создания активов.

ISO 19650–3:2020 Organization of information about construction works – Information management using building information modelling – Part 3: Operational phase of assets (Организация и оцифровка информации о строительных объектах и работах в области гражданского строительства, включая информационное моделирование строительных объектов (BIM). Управление информацией с использованием информационного моделирования строительных объектов. Часть 3. Этап эксплуатации активов).

Примечание – При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов и классификаторов по ежегодно издаваемому информационному указателю «Документы по стандартизации» по состоянию на текущий год и соответствующим ежемесячно издаваемым информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) документом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

**3 Термины и определения**

В настоящем стандарте применяются следующие термины и определения:

**3.1** **Актив** (asset): Предмет, вещь или сущность, которые имеют потенциальную или фактическую ценность для организации.

Примечания

1. Актив может быть фиксированным, мобильным или движимым. Это может быть отдельный объект установки, транспортное средство, система подключенного оборудования, пространство внутри сооружения, земельный участок, участок инфраструктуры, весь строительный объект или портфель активов, включая связанные с ним земли и водоснабжение. Он также может содержать информацию в цифровом или печатном виде.

2. Стоимость актива может меняться на протяжении всего срока его службы, и актив все еще может иметь ценность в конце срока своей службы. Ценность может быть материальной, нематериальной, финансовой или нефинансовой.

Взято из ISO 55000:2014, пункт 3.2.1, модифицировано – Примечания 1, 2 и 3 были удалены; добавлены новые Примечания 1 и 2.

**3.2** **Многолюдное место** (crowded place): Местоположение или среда доступное представителям общественности, которое может считаться более подверженным риску террористической атаки в силу концентрации людей или характера местности.

Примечания:

1. Места массового скопления людей могут включать: спортивные стадионы, арены, площадки для фестивалей и музыкальные площадки; отели и рестораны; пабы, клубы, бары и казино; центральные улицы, торговые центры и рынки; достопримечательности для посетителей; кинотеатры и театры; школы и университеты; больницы и культовые сооружения; коммерческие центры; и транспортные узлы. Они также могут включать мероприятия и общественные места, такие как парки и площади.

2. Многолюдное место не обязательно будет переполнено постоянно – концентрация людей может варьироваться и может быть временной, как в случае спортивных мероприятий или фестивалей под открытым небом.

**3.3 Метаданные** (metadata): Данные о данных.

**3.4. Потребность знать** (need-to-know): Легитимное требование потенциального получателя информации знать, иметь доступ или обладать конфиденциальной информацией (пункт 3.11).

**3.5 Склонность к риску** (risk appetite): Размер и тип риска, который организация готова принять или сдерживать.

Примечание – Взято из ISO 22300:2018, пункт 3.202.

**3.6 Защищенность** (safety): Состояние относительной свободы от угрозы (пункт 3.13) или вреда, причиненного случайными, непреднамеренными действиями или событиями.

**3.7 Безопасность** (security): Состояние относительной свободы от угрозы (пункт 3.13) или вреда, причиненного преднамеренными, нежелательными, враждебными или злонамеренными действиями.

**3.8 Нарушение безопасности** (security breach): Повреждение или несоблюдение безопасности (пункт 3.7).

Примечание – Взято из ISO 14298:2013, пункт 3.30.

**3.9 Инцидент безопасности** (security incident): Подозрительное действие или обстоятельство, угрожающее безопасности (пункт 3.7).

**3.10 Ориентированный на безопасность** (security-minded): Понимание и регулярное применение надлежащих и соразмерных мер безопасности (пункт 3.7) в любой бизнес-ситуации для предотвращения и/или пресечения враждебного, злонамеренного, мошеннического и преступного поведения или деятельности.

**3.11 Конфиденциальная информация** (sensitive information): Информация, потеря, неправильное использование, изменение или несанкционированный доступ к которой могут:

– отрицательно повлиять на приватность, безопасность (пункт 3.7) или защищённость (пункт 3.6) физического лица или физических лиц;

– привести к компрометации интеллектуальной собственности или коммерческой тайны организации;

– нанести коммерческий или экономический ущерб организации или государству; и/или

– поставить под угрозу безопасность, внутренние и внешние национальные интересы.

**3.12 Остаточный риск** (residual risk): Риск, который остается после внедрения мер контроля.

Примечание – Взято из ISO 16530‑1:2017, пункт 3.52.

**3.13 Угроза** (threat): Потенциальная причина инцидента, который может привести к причинению вреда.

**3.14 Высшее руководство** (top management): Лицо или группа лиц, которые руководят и контролируют организацию на самом высоком уровне.

Примечания:

1. Высшее руководство имеет право делегировать полномочия и предоставлять ресурсы внутри организации.

2. В контексте настоящего стандарта управление следует рассматривать как функцию, а не как деятельность.

Взято из ISO 9000:2015, пункт 3.1.1, модифицировано – Примечания 2 и 3 были удалены; добавлено новое Примечание 2.

**3.15 Уязвимость** (vulnerability): Недостаток, который можно использовать для причинения вреда.

**4 Установление необходимости подхода, ориентированного на безопасность с использованием процесса оценки конфиденциальности**

**4.1 Проведение процесса оценки конфиденциальности**

Процесс проведения оценки конфиденциальности изложен в пунктах 4.2–4.4 настоящего стандарта.

**4.2 Понимание диапазона рисков безопасности**

**4.2.1** Высшее руководство организации, участвующей в:

a) инициировании проекта по созданию нового актива (ов), продукта (ов) или модификации/улучшении существующего;

b) управлении, эксплуатации, переориентации или распоряжении активом (активами); и/или

c) предоставление услуги (услуг) на основе активов.

определяет диапазон рисков безопасности, возникающих в результате повышения доступности информации, интеграции услуг и систем и усиления зависимости от систем, основанных на технологиях.

**4.2.2** Информация о типах рисков безопасности, которые следует учитывать, содержится в Приложении A.

**4.2.3** В случае участия двух или более организаций, высшее руководство каждой организации (пункт 4.2.1) должно действовать скоординированным образом.

Примечание – Такое объединение нескольких организаций может произойти в городе/сообществе, крупном многоцелевом комплексе или при обеспечении транспортной системы.

**4.3 Идентификация организационных особенностей**

**4.3.1** Принимая во внимание диапазон существующих рисков безопасности, организация (организации), упомянутая в пунктах 4.2.1 и 4.2.3 должна (должны) определить, следует ли считать инициативу, проект, актив, продукт или услугу, а также любую связанную с ними информацию, включая планируемую или существующую, полностью или частично конфиденциальной.

Примечание – В настоящем стандарте упоминание термина «организация (организации)» относится к организации (организациям) упомянутым в пунктах 4.2.1 и 4.2.3.

**4.3.2** Построенный актив должен считаться конфиденциальным, в целом или частично, если он:

a) включает важнейшую национальную инфраструктуру, определенную местным исполнительным или центральным государственным органом;

b) выполняет оборонную, правоохранительную или дипломатическую функцию, или функцию по обеспечению национальной безопасности;

c) является коммерческим участком, связанным с созданием, обработкой, торговлей или хранением ценных материалов, валюты, фармацевтических препаратов, химических веществ, нефтехимических продуктов или газов, а также предоставлением или производством средств для производства этих материалов;

d) представляет собой достопримечательность, национально значимый объект или многолюдное место;

e) используется или планируется к использованию для проведения мероприятий, имеющих важное значение для безопасности.

Примечание – Тот факт, что построенный актив не подпадает под описанные критерии, не исключает применения более высокого уровня безопасности, если организация (организации) стремится к этому.

**4.3.3** Актив, продукт или услуга также должны считаться конфиденциальными, если существует достаточный риск того, что они используются или могут быть использованы для существенного нарушения целостности, защищенности, безопасности и/или устойчивости актива, продукта или услуги или их способности функционировать.

**4.3.4** Актив, продукт или услуга также считаются конфиденциальными, если риск для защищенности, безопасности и/или приватности отдельных лиц или сообществ или их персональной информации превышает склонность организации (организаций) к риску.

**4.3.5** Если существует какая-либо неопределенность относительно того, является ли инициатива, проект, актив, продукт или услуга конфиденциальными, организация (организации) должна (должны) обратиться за консультацией к соответствующим экспертам по безопасности, которые могут продемонстрировать компетентность в требуемых областях.

Примечание – Информация о получении соответствующих рекомендаций по безопасности содержится в Приложении A.

**4.4 Установление любых конфиденциальных данных третьих сторон**

**4.4.1** Оценка инициативы, проекта, актива, продукта или услуги также должна учитывать, будет ли получен или уже получен доступ к информации о других организациях, их активах, продуктах или услугах, которая тем или иным образом не является общедоступной.

Примечание – Например, информация, которая не является общедоступной и может быть конфиденциальной, может быть получена в результате физических обследований подземных сооружений, инженерных сетей и систем расположенных на частном земельном участке.

**4.4.2** Организация (организации), если это не запрещено по коммерческим или локальным соображениям, консультируется с привлекаемой организацией (организациями), чтобы установить, является ли какая-либо информация конфиденциальной, и в этом случае, какие меры необходимо применять для ее сбора, обработки, хранения, обмена, удаления и изменения.

**4.5 Запись результатов оценки конфиденциальности**

Организация (организации) регистрирует и сохраняет результаты каждого процесса оценки конфиденциальности, в том числе в тех случаях, когда конфиденциальность не выявлена, и признает (признают), что результат сам по себе может быть конфиденциальным.

**4.6 Обзор оценки конфиденциальности**

**4.6.1** Организация (организации) должна (должны) создать подходящий механизм для проведения периодических и основанных на событиях обзоров, которые проверяют, произошли ли какие-либо изменения в конфиденциальности инициативы, проекта, актива, продукта или услуги, будь то по политическим, экономическим, социальным, технологическим, правовым или экологическим причинам.

**4.6.2** Обзор также должен проводиться, когда в инициативе, проекте, активе, продукте или услуге происходят существенные изменения, в том числе касающиеся:

a) владения, использования или размещения построенного актива;

b) процессов или систем, используемых при управлении построенным активом или производства актива или продукта;

c) информации, собранной, обработанной и/или сохраненной;

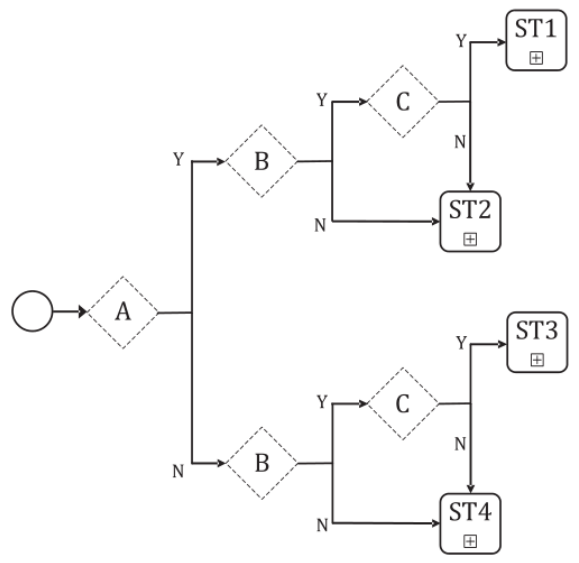
d) оказанной услуги; или

e) контекста безопасности.

**4.6.3** Дополнительные обзоры, основанные на событиях, должны проводиться, когда происходят события, выявляющие уязвимости, которые ранее не ожидались.

**4.7 Определение необходимости применения подхода, ориентированного на безопасность**

Организация (организации) должна применять процесс сортировки безопасности, описанный на рисунке 3, чтобы определить, требуется ли подход, ориентированный на безопасность, в отношении инициативы, проекта, актива, продукта или услуги.



**Условные обозначения:**

|  |  |
| --- | --- |
| A | считается ли инициатива, проект, актив, продукт или услуга, а также любая связанная с ними информация, включая планируемую или существующую, полностью или частично, конфиденциальной (см. пункт 4.3)? |
| B | будет ли получен или уже получен доступ к информации о другой организации, ее активах, продуктах или услугах, которая тем или иным образом не является общедоступной (см. пункт 4.4.1)? |
| C | считается ли информация о другой организации, ее активах, продуктах или услугах конфиденциальной (см. пункт 4.4.2)? |
| Y | да |
| N | нет |
| ST1 | защитите конфиденциальную информацию, касающуюся инициативы, проекта, активов, продукта или услуги, а также конфиденциальную информацию третьих сторон, применив разделы 5–9 настоящего стандарта |
| ST2 | защитите конфиденциальную информацию об инициативе, проекте, активе, продукте или услуге, применив разделы 5–9 настоящего стандарта |
| ST3 | защитите конфиденциальную информацию третьих лиц, применив разделы 5–9 настоящего стандарта и защитите любую конфиденциальную коммерческую и персональную информацию |
| ST4 | защитите любую конфиденциальную коммерческую и персональную информацию |
| Примечание – ST – это сокращенный термин для «сортировки безопасности» | |

**Рисунок 3 – Процесс сортировки безопасности**

**4.8 Запись результатов применения процесса сортировки безопасности**

Организация (организации) должна (должны) регистрировать результат (ST1, ST2, ST3 или ST4) применения процесса сортировки безопасности для каждой инициативы, проекта, актива, продукта или услуги, к которым он применяется, в том числе в тех случаях, когда нет выявленной необходимости в подходе, ориентированном на безопасность, помимо защиты конфиденциальной коммерческой и персональной информации.

**4.9** **Потребность в подходе, ориентированном на безопасность**

Если инициатива, проект, актив, продукт или услуга:

a) был определен как конфиденциальный, полностью или частично; и/или

b) будет содержать информацию третьих лиц, которая была определена как конфиденциальная,

высшее руководство организации (организаций) должно, в соответствии с требованиями настоящего стандарта, разработать и внедрить соответствующий и соразмерный подход, ориентированный на безопасность.

**4.10** **Отсутствие потребности в подходе, ориентированном на безопасность**

В тех случаях, когда инициатива, проект, актив, продукт или услуга не считаются конфиденциальными и не имеют доступа к иной конфиденциальной информации третьих лиц, организация (организации) должна (должны) рассмотреть вопрос о том, можно ли извлечь бизнес-выгоды из применения подхода, ориентированного на безопасность.

Примечания:

1. Разумно, чтобы организации предпринимали надлежащие шаги для минимизации угроз, возникающих в результате мошенничества и другой преступной деятельности, а также в результате инцидентов кибербезопасности.

2. Вполне вероятно, что в соответствии с условиями назначения или законодательством потребуются базовые меры безопасности, касающиеся персональной информации и коммерческой информации.

3. Если организация (организации) не желает принять какой-либо более высокий уровень безопасности, нет необходимости в применении требований разделов 5–9 настоящего стандарта к инициативе, проекту, активу, продукту или услуге в том виде, в каком они оцениваются в настоящее время.

**5 Инициирование подхода, ориентированного на безопасность**

**5.1 Установление системы управления, подотчетности и ответственности за подход ориентированный на безопасность**

**5.1.1** Если организация разрабатывает подход, ориентированный на безопасность, высшее руководство должно определить лицо на уровне высшего руководства, ответственное за применяемый подход, ориентированный на безопасность.

**5.1.2** Если две или более организации разрабатывают совместный подход, ориентированный на безопасность, высшее руководство каждой организации должно создать официальный механизм для:

a) создания требуемой структуры управления, обеспечения ее юридического оформления и того, чтобы отношения данной структуры с соответствующими организациями были официально задокументированы и согласованы;

b) согласования стороны или сторон, которые будут руководить разработкой подхода, и где эта функция руководства распределена между организациями, обеспечивая четкость в отношении ответственности и обязанностей;

c) назначения ответственных лиц, которые будут нести ответственность за применяемый подход, ориентированный на безопасность; и

Примечание – Физические лица назначаются для осуществления законных прав и выполнения обязательств своей соответствующей организации.

d) обзора и, при необходимости, обновление структуры управления и назначений.

Примечание – Согласованный совместный подход, ориентированный на безопасность, является более надежным, чем подход, при котором организации работают изолированно.

**5.1.3** Организация (организации), применяющая подход, ориентированный на безопасность, должна определить лицо (лиц), ответственное (ответственных) за:

a) предоставление целостного представления об угрозах безопасности и уязвимостях, возникающих в результате использования и опоры на информационно-коммуникационные технологии, имеющие отношение к инициативе, проекту, активу, продукту или услуге;

b) предоставление рекомендаций и указаний по устранению возникающих рисков безопасности;

c) управление разработкой стратегии безопасности или, если у организации уже есть стратегия безопасности, управление включением записей о дополнительных рисках безопасности и мерах по их снижению, возникающих в результате использования и опоры на информационно-коммуникационные технологии, имеющие отношение к инициативе, проекту, активу, продукту или услуге (см. раздел 6);

d) управление разработкой и оказание помощи в реализации плана управления безопасностью или, если у организации уже есть план управления безопасностью, управление внедрением в него соответствующих дополнительных политик и процессов (см. раздел 7);

e) помощь во внедрении необходимых требований по безопасности в любую документацию по закупкам и назначениям;

f) поощрение культуры, ориентированной на безопасность, с тем чтобы все сотрудники понимали свои обязанности по обеспечению безопасности и вели себя соответствующим образом;

g) информирование соответствующих третьих сторон о соответствующих аспектах политики и процессов безопасности;

h) консультирование по вопросам необходимости и проведения обзора и аудита соответствующих политик и процессов безопасности;

i) консультирование по вопросам необходимости и (там, где это уместно и необходимо) проведения или ввода в эксплуатацию испытаний соответствующих мер безопасности; и

j) обращение за консультацией (там, где это уместно и необходимо) к соответствующим службам безопасности, которые могут продемонстрировать компетентность в требуемых областях, и предоставить дополнительные рекомендации.

**5.1.4** Лица, выполняющие действия, перечисленные в пункте 5.1.3, должны иметь четкие указания по отчетности перед лицом, ответственным за безопасность в своей организации.

Примечание – Эти функции могут выполняться квалифицированным и опытным специалистом, который может выполнять контроль или отвечать за безопасность и другие обязанности в организации, или может быть подходящим экспертом, нанятым организацией.

**5.1.5** Должно быть приемлемо, чтобы конкретные задачи или обязанности по обеспечению безопасности делегировались на ежедневной основе другими лицами (например, безопасность персонала – персоналу, кибербезопасность – ИТ-менеджеру, а безопасность активов или физическая безопасность – менеджеру активов или менеджеру объектов). Тем не менее, лицо (лица), определяемое как выполняющее действия, перечисленные в пункте 5.1.3, остается ответственным за операционную эффективность каждого из этих аспектов безопасности.

**5.2 Начало разработки подхода, ориентированного на безопасность**

**5.2.1** Для планируемой инициативы, проекта, актива, продукта или услуги подход, ориентированный на безопасность, должен быть разработан как можно раньше на этапах планирования.

Примечание – Информация, касающаяся разработки, которая становится общедоступной, может представлять интерес для разведки враждебной стороны с самых ранних стадий процесса проектирования.

**5.2.2** Если конфиденциальная инициатива, проект, актив, продукт или услуга уже существуют, подход, ориентированный на безопасность, должен быть разработан как можно скорее и должен учитывать степень, в которой информация уже находится в общественном доступе.

**5.2.3** Если проект относится к этапу поставки актива с использованием BIM, подход, ориентированный на безопасность, должен быть разработан в соответствии с требованиями, описанными в ISO 19650–2.

**5.2.4** Если деятельность относится к этапу эксплуатации актива с использованием BIM, подход, ориентированный на безопасность, должен быть разработан в соответствии с требованиями, описанными в ISO 19650–3.

**6 Разработка стратегии безопасности**

**6.1 Общие положения**

**6.1.1** Организация (организации) должна (должны) разработать и поддерживать стратегию безопасности, которая должна включать:

a) запись о результатах применения процесса сортировки безопасности;

b) механизмы управления, подотчетности и ответственности для подхода, ориентированного на безопасность;

c) оценка конкретных рисков для безопасности организации (организаций), возникающих в связи с большей доступностью информации, интеграцией услуг и систем, и возросшей зависимостью от систем, основанных на технологиях (см. пункт 6.2);

d) потенциальные меры по снижению рисков для устранения этих рисков безопасности и меры по снижению рисков, которые должны быть реализованы;

e) краткое описание допустимых рисков безопасности и остаточных допустимых рисков безопасности (см. пункт 6.4); и

f) механизмы пересмотра и обновления стратегии безопасности (см. пункт 6.5).

Примечание – Принципы, структура и процесс управления рисками на общем уровне предусмотрены стандартом ISO 31000.

**6.1.2** Стратегия безопасности должна учитывать требования законодательства и стандарты, которые были определены как имеющие отношение к инициативе, проекту, активу, продукту или услуге.

**6.1.3** Стратегия безопасности должна быть утверждена высшим руководством организации (организаций).

**6.1.4** Доступ к любой части стратегии безопасности, которая определяет аспекты конфиденциальности инициативы, проекта, актива, продукта или услуги или детализирует выявленные риски безопасности, должен управляться на основе строгой потребности знания о том, что вся такая информация подлежит мерам безопасности, соответствующим уровню риска, в отношении ее создания, обработки и хранения.

**6.2 Оценка рисков безопасности**

**6.2.1** Организация (организации) должна (должны) оценить конкретные риски безопасности, возникающие в связи с большей доступностью информации, интеграцией услуг и систем и возросшей зависимостью от систем, основанных на технологиях, путем оценки:

a) потенциальных угроз;

b) потенциальных уязвимостей;

c) характера вреда, который может быть причинен инициативе, проекту, активу, продукту или услуге, а также персоналу, гражданам и окружающей среде; и

d) вероятности того, что уязвимость будет использована и вызовет это воздействие.

Примечание – При оценке рисков безопасности может быть целесообразно использовать тот же подход к оценке рисков, который применяется в других подразделениях организации.

**6.2.2** В тех случаях, когда информация уже опубликована, при оценке рисков безопасности следует учитывать, что после публикации информации в Интернете или иного публичного доступа ее практически невозможно удалить, уничтожить, нарушить или защитить все ее копии.

**6.2.3** В соответствующих случаях оценка рисков безопасности должна включать риски безопасности, связанные с доступом к информации других организаций, которая тем или иным образом не является общедоступной.

**6.3 Разработка мер по снижению рисков безопасности**

**6.3.1** Организация (организации) должна (должны) определять и регистрировать возможные меры по смягчению последствий для каждого выявленного риска безопасности или комбинации выявленных рисков.

**6.3.2** При определении и регистрации возможных мер по смягчению последствий, организация (организации) должна (должны) учитывать кадровые, физические и технические средства контроля безопасности и требования, касающиеся управления информацией.

Примечания:

1. Взаимодействие между персоналом, физическими и техническими средствами контроля может быть использовано авторами угроз, если связи между этими областями не были изучены.

2. Разработанные меры по смягчению последствий также могут быть направлены на сохранение или защиту коммерческой, экономической и социальной ценности.

3. Информация о типах средств контроля безопасности и факторах управления информацией содержится в Приложении В.

**6.3.3** При оценке каждой потенциальной меры по смягчению последствий, организация (организации) должна (должны) учитывать:

a) стоимость мер по смягчению последствий и их реализацию;

b) снижение риска, которое может быть достигнуто, и уровень остаточного риска;

c) прогнозируемое влияние мер по смягчению риска последствий на стоимость;

d) другое влияние, которое может оказать мера по смягчению последствий на актив (которое может включать удобство использования, эффективность и внешний вид);

e) потенциал этой меры при создании дополнительных уязвимостей; и

f) обеспечивает ли эта мера какие-либо другие преимущества для бизнеса.

Примечание – Преимущества для бизнеса могут включать снижение общего бизнес-риска и обеспечение понимания стоимости активов, включая информацию.

**6.3.4** Организация (организации) должна (должны) использовать результаты оценки для определения того, какие меры по смягчению последствий, если таковые имеются, принимаются.

Примечание – Соразмерная мера по смягчению последствий – это прагматичная, целесообразная и экономически эффективная мера.

**6.4 Документирование остаточных и допустимых рисков безопасности**

**6.4.1** После разработки мер по снижению уровня безопасности организация (организации) должна (должны) идентифицировать и регистрировать любые остаточные риски безопасности.

**6.4.2** Организация (организации) должна (должны) продолжать процессы оценки риска безопасности и разработки мер по снижению риска безопасности в отношении этих рисков безопасности до тех пор, пока не будет достигнут момент, когда склонность к риску отдельной организации или склонность к риску группы организаций не будет оптимальной.

**6.4.3** Организация (организации) должна (должны) документировать допустимые риски безопасности.

**6.5 Обзор стратегии безопасности**

**6.5.1** Организация (организации) должна (должны) создать подходящий механизм для проведения периодических и основанных на событиях обзоров стратегии безопасности, включая эффективность действующих мер по смягчению последствий, для проверки того, что она соответствует поставленным целям.

**6.5.2** Обзоры, основанные на событиях, должны проводиться, когда происходят политические, экономические, социальные, организационные, технологические, правовые или экологические изменения, которые могут существенно повлиять на инициативу, проект, актив, продукт или услугу, а также связанную с ними информацию или события, которые выявляют уязвимости, которые ранее не ожидались.

**6.5.3** При проведении обзоров должны учитываться потенциальные последствия для существующих назначений, на которые могут повлиять значительные изменения в мерах по смягчению последствий, особенно в тех случаях, когда они представляют собой изменение сферы применения.

**6.5.4** После проверки стратегия безопасности должна быть обновлена с учетом любых изменений угроз, уязвимостей, возникающих рисков безопасности и/или мер по снижению рисков безопасности.

**6.5.5** Возникновение каждой активности должно регистрироваться и сохраняться как часть стратегии безопасности.

**6.5.6** Доступ к любой части обзора, в которой определяются аспекты конфиденциальности инициативы, проекта, актива, продукта или услуги или подробно описываются выявленные риски безопасности, должен осуществляться на основе строгой потребности знания о том, что при этом вся такая информация подлежит мерам безопасности, соответствующим уровню риска, в отношении ее создания, распределения, использования, хранения, удаления и уничтожения.

**7 Разработка плана управления безопасностью**

**7.1 Общие положения**

**7.1.1** Организация (организации) должна (должны) разработать, поддерживать и внедрять план управления безопасностью, который позволяет согласованным мерам по смягчению последствий, изложенным в стратегии безопасности, осуществляться последовательным и целостным образом.

**7.1.2** Управление безопасностью должно, при необходимости, иметь перекрестные ссылки на другие политики и процессы управления безопасностью, и соответствующие политики и процессы, которые существуют в организации (организациях)

**7.1.3** План управления безопасностью должен содержать, в отношении организации (организаций) и ее команды поставки:

a) политики, которые устанавливают бизнес-правила, связанные с безопасностью, вытекающие из согласованных мер по смягчению последствий;

b) процессы, вытекающие из политики безопасности, и рекомендации по их последовательной реализации;

c) требования по информационной безопасности с подробным описанием информации, которая должна рассматриваться как конфиденциальная, а также политики и процессы ее создания, распределения, использования, хранения, удаления и уничтожения;

d) требования, касающиеся предоставления информации третьим лицам (см. пункт 7.2);

e) требования к логистической безопасности там, где это применимо (см. пункт 7.3);

f) план управления нарушениями безопасности/инцидентами (см. раздел 8);

g) подробную информацию о подотчетности и ответственности за реализацию различных аспектов плана обеспечения безопасности (см. пункт 7.4);

h) требования к мониторингу и аудиту, включая проверку действующих мер безопасности (см. пункт 7.5); и

i) механизмы пересмотра и обновления плана управления безопасностью (см. пункт 7.6).

Примечание – Любые пробелы или упущения в плане управления безопасностью снизят эффективность стратегии безопасности и увеличат риск нарушения безопасности или инцидента.

**7.1.4** План управления безопасностью должен использоваться для информирования о требованиях по информационной безопасности, включенных в любые документы о закупках и назначениях (см. раздел 9).

**7.2 Предоставление информации третьим лицам**

**7.2.1** План управления безопасностью должен устанавливать требования организации (организаций) для проведения оценки до предоставления и/или публикации новой, измененной или существующей информации или информационной модели полностью или частично.

**7.2.2** Такая оценка должна быть способна реагировать (где это применимо) на:

a) необходимость соблюдения организацией нормативных и уставных процессов;

b) запрос на информацию, полученную организацией, на которую распространяются положения законодательства о публичном доступе или прозрачности; и

c) необходимость иметь материалы, которые могут быть использованы на общественных и профессиональных мероприятиях, в маркетинговых материалах, в технических, академических или других публикациях и веб-сайтах.

**7.2.3** Оценка должна учитывать (насколько это разумно и практически осуществимо), что информация или информационная модель полностью или частично:

a) содержит или позволяет выводить конфиденциальную информацию, включая информацию об уязвимостях, об инициативе, проекте, активе, продукте, услуге, отдельном лице или группе/сообществе;

b) при объединении с существующими общими или опубликованными материалами позволяет выводить конфиденциальную информацию; и

c) способствует (там, где это применимо) определению характера использования актива (активов) и/или образа жизни отдельных лиц или групп/сообществ, которые тем, иным образом не являются общедоступными.

Примечание – Руководство по областям, охватываемым этим типом оценки, содержится в Приложении С.

**7.2.4** Если в результате оценки будет установлено, что какое-либо из этих обстоятельств имеет место, организация (организации) должна (должны) применять надлежащий и соразмерный подход, основанный на оценке рисков, к обмену и/или публикации этой информации.

Примечание – Рекомендации по потенциальным мерам, которые могут быть использованы для снижения рисков безопасности, приведены в Приложении C.

**7.2.5** Доступ к любой части оценки, в которой детализируется конфиденциальная информация, должен управляться на основе строгой потребности знания о том, что при этом информация, содержащаяся в ней, подлежит соответствующим мерам безопасности в отношении ее создания, распределения, использования, хранения, удаления и уничтожения.

**7.3 Материально-техническая безопасность**

**7.3.1** В соответствующих случаях план управления безопасностью должен предусматривать надлежащие и соразмерные меры безопасности в отношении спецификации, закупок, проектирования, производства, транспортировки, установки и ввода в эксплуатацию любых конфиденциальных активов.

Примечание – При разработке этих мер можно обратиться за консультацией к специалистам.

**7.3.2** Организация (организации) должна (должны) рассмотреть:

a) сроки установки любых конфиденциальных активов или систем, связанных с безопасностью, чтобы, по возможности, доступ к этим активам или областям был ограничен теми, кто наделен соответствующим легитимным правом;

b) принятие надлежащих и соразмерных мер безопасности в отношении любых конфиденциальных активов и систем, которые по материально-техническим причинам должны быть установлены раньше, чем обычно было бы желательно.

c) осуществление надлежащих и соразмерных мер по ограничению или срыву успеха физической разведки враждебной стороны.

**7.4 Управление подотчетностью и ответственностью за безопасность**

Каждая политика в плане управления безопасностью должна определять лицо (лиц), выполняющее функцию (функции) управления безопасностью, которые подотчетны и отвечают за ее реализацию, управление, мониторинг и обзор.

**7.5 Мониторинг и аудит**

**7.5.1** В плане управления безопасностью должны быть изложены надлежащие и соразмерные меры по мониторингу, аудиту и тестированию, которые должны проводиться на протяжении всего жизненного цикла инициативы, проекта, актива, продукта или услуги, которые должны включать оценку, как минимум, на основе подхода к выборке, основанного на риске:

a) осуществление всех аспектов плана обеспечения безопасности; и

b) соответствие любой команды поставки всем соответствующим аспектам плана управления безопасностью.

Примечания:

1. Необходимо найти баланс между официальной верификацией, включающей назначенные сторонние аудиты, и системой проверки, основанной на уважении/доверии.

2. Там, где это применимо, соответствие команды поставки всем соответствующим аспектам плана управления безопасностью может быть частью анализа способностей и возможностей, определенного в ISO 19650–1.

3. Мониторинг и аудит плана управления безопасностью могут основываться на таких стандартах, как ISO 19011.

**7.5.2** План управления безопасностью требует, чтобы только лица, обладающие соответствующей квалификацией и опытом, выполняли эту работу по мониторингу и аудиту.

**7.5.3** Организация (организации) может делегировать определенную ответственность за проверку соответствия (в рамках команды поставки) назначенной стороне, но должна сохранять ответственность за общую эффективность средств контроля безопасности.

**7.6 Обзор плана обеспечения безопасности**

**7.6.1** Организация (организации) должна (должны) создать подходящий механизм для проведения периодических и основанных на событиях проверок плана управления безопасностью, включая требования по информационной безопасности и план управления нарушениями безопасности/инцидентами, чтобы убедиться, что он остается пригодным для целей.

**7.6.2** Обзоры, основанные на событиях, должны проводиться после пересмотра стратегии безопасности, в случае нарушения безопасности или инцидента, или когда происходят политические, экономические, социальные, организационные, технологические, правовые или экологические изменения, которые могут существенно повлиять на:

a) типы нарушений/инцидентов безопасности, которые могут произойти;

b) процесс, которому необходимо следовать, включая необходимость сбора доказательств судебной экспертизы; и

c) меры по обеспечению непрерывности бизнеса и меры по восстановлению.

**7.6.3** Обзоры должны учитывать потенциальное влияние на существующие назначения любых изменений в политике и процессах, особенно в тех случаях, когда они представляют собой изменение сферы применения.

**7.6.4** После проверки план управления безопасностью должен быть обновлен для отражения любых изменений, а также для устранения любых выявленных пробелов и недостатков, которые снижают способность плана обеспечивать требуемый уровень снижения рисков безопасности.

**7.6.5** Изменения в плане управления безопасностью должны быть доведены до сведения организации (организаций) и назначенных сторон.

**7.6.6** Событие по каждой проверке должно регистрироваться и сохраняться как часть плана управления безопасностью.

**8 Разработка плана управления нарушениями безопасности/инцидентами**

**8.1 Общие положения**

**8.1.1** Организация (организации) должна (должны) создать и поддерживать план управления нарушениями безопасности/инцидентами в рамках плана управления безопасностью, который должен включать:

a) оценку типов возможных нарушений/инцидентов безопасности и потенциальных рисков, которые могут возникнуть, влияющих на организацию (организации), ее функции, активы и репутацию, персонал и третьи стороны;

b) процесс, который необходимо выполнить при обнаружении нарушения безопасности/инцидента, включая тот, который едва не произошел (см. пункт 8.2);

c) меры по обеспечению непрерывности бизнеса и меры по восстановлению, обеспечивающие тот же уровень безопасности, что и системы, используемые ежедневно, включая (где это применимо) сбор доказательств для правоохранительных целей (см. пункт 8.3).

**8.1.2** Части плана управления нарушениями безопасности/инцидентами могут быть охвачены другими существующими планами или конкретными действиями национальной специфики, и в этом случае на эти планы или действия должны быть даны перекрестные ссылки.

**8.1.3** Части плана управления нарушениями безопасности/инцидентами, в которых регистрируются риски для организации (организаций), должны управляться на основе строгой необходимости, при этом информация, содержащаяся в этих частях, подлежит соответствующим мерам безопасности в отношении ее создания, распределения, использования, хранения, удаления и уничтожения.

**8.2 Обнаружение нарушения безопасности или инцидента**

Организация (организации) должна (должны) определить шаги, которые необходимо предпринять в случае обнаружения нарушения безопасности или инцидента, которые должны включать:

a) лица или роли, с которыми необходимо немедленно связаться, и их контактные данные;

b) процессы, используемые для выявления заинтересованных сторон;

c) механизмы уведомления заинтересованных сторон и подлежащая предоставлению информация; и

d) обработку данных любых третьих сторон, регулирующих органов, средств массовой информации или общественных интересов в случае инцидента с нарушением безопасности.

**8.3 Сдерживание и восстановление**

Организация (организации) должна (должны) определить шаги, которые необходимо предпринять в случае обнаружения нарушения безопасности/инцидента, содержащие и устраняющие последствия события, которые включают:

a) меры по уменьшению дальнейшего ущерба или убытков;

b) оценку того, что было потеряно, скомпрометировано, повреждено или искажено;

c) обстоятельства, при которых требуется сбор доказательств для правоохранительных целей, и подход; и

d) меры по обеспечению готовности к судебной экспертизе, необходимые для обеспечения (при необходимости) сбора криминалистической информации об инциденте для использования правоохранительными органами и/или детального анализа первопричин инцидента.

В обстоятельствах, когда необходимо собрать доказательства для правоохранительных целей, все доказательства (т. е. как физические, так и цифровые), которые могут помочь расследованию установить причину события и виновных, должны быть сохранены и собраны до принятия любых мер по восстановлению, если только непосредственная необходимость в таких действиях не является критической для жизнедеятельности.

Примечание – Важно, чтобы криминалистические доказательства были собраны до принятия мер по восстановлению, поскольку эти действия могут уничтожить или исказить цифровые криминалистические доказательства.

**8.4 Просмотр после нарушения безопасности или инцидента**

**8.4.1** После первоначальных действий по сдерживанию и восстановлению, организация (организации) должна (должны) провести оценку текущего риска. Эта оценка должна изучить причины события, определить потенциальные контрмеры и оценить остаточный риск, а также любой потенциальный новый или усиленный риск, возникающий в результате события.

**8.4.2** Соответствующие политики и процессы должны быть обновлены, чтобы отразить результаты оценки и предотвратить или снизить риск повторного возникновения.

**8.4.3** Организация (организации) должна (должны) требовать (где это применимо), чтобы соответствующие члены ее команды поставки сотрудничали с ней для проведения надлежащей и соразмерной оценки события после инцидента и реагирования.

**9 Работа с назначенными сторонами**

**9.1 Работа вне официальных назначений**

**9.1.1** Организация (организации) должна (должны) заключать соглашения об обмене информацией или эквивалентные соглашения при работе вне официальных назначений (например, во время тендера), если будет предоставлен доступ к конфиденциальной информации.

Примечание – Дополнительная информация о соглашениях об обмене информацией содержится в Приложении D.

**9.1.2** Соглашение об обмене информацией или его эквивалент должны включать требования организации (организаций) к хранению, удалению и уничтожению конфиденциальной информации.

**9.1.3** Когда процесс назначения во время тендера требует разглашения конфиденциальной информации, организация (организации) должна (должны) применять надлежащие и соразмерные меры защиты и/или отдельные процессы, обеспечивая при этом наличие достаточной информации.

**9.1.4** Организация (организации) в рамках процесса отбора назначенной стороны должна (должны) оценить всю тендерную документацию, чтобы установить, каким образом предполагается обеспечить соблюдение требований по информационной безопасности, изложенных в плане управления безопасностью.

**9.1.5** Организация (организации) должна (должны) оценить понимание, возможности, компетентность и опыт организаций в области безопасности для назначения, а также любые требования к обучению, наставничеству и поддержке в области безопасности.

**9.2 Меры, содержащиеся в документации о назначении**

**9.2.1** Организация (организации) должна (должны) управлять рисками безопасности своей команды поставки, включив в документацию о назначении положения, которые поддерживают все соответствующие политики и процессы безопасности, содержащиеся в плане управления безопасностью, включая требования, предъявляемые к члену команды поставки по завершении назначения.

**9.2.2** Организация (организации) должна (должны) подробно описать распределение функций информационной безопасности для команды поставки, включая требование о том, чтобы безопасность сохранялась на подотчетных уровнях в команде поставки, с соответствующим делегированием ответственности, чтобы можно было обеспечить эффективное управление.

**9.2.3** В соответствующих случаях положения должны включать применение тех же требований, которые содержатся в документации о назначении для назначенных сторон, которые назначаются непосредственно в организацию (организации), через уровни дополнительных назначений.

**9.2.4** В тех случаях, когда требуется соблюдение конкретных стандартов безопасности (например, обеспечение конкретных мер физической или кибербезопасности в соответствии с определенным стандартом), они должны быть четко указаны в документации о назначении, наряду с любой ожидаемой независимой инспекцией или верификацией третьей стороной.

**9.2.5** Для обработки нарушений/инцидентов безопасности, вызванных профессиональным консультантом, подрядчиком или назначенной стороной, в документации о назначении должны быть четкие положения для сообщения организации (организациям) о нарушении/инциденте безопасности и для оказания помощи в расследовании и последующих действиях.

**9.2.6** Меры, включенные в документацию о назначении, должны содержать положения, позволяющие организации (организациям) анализировать меры безопасности и соблюдение соответствующих политик и процессов безопасности на любом уровне в соответствующей команде поставки.

**9.2.7** Организация (организации) должна (должны) включить в документацию о назначении пункт, позволяющий вносить коррективы в ответ на изменения в политической, законодательной или нормативной среде, подлежащие внедрению.

**9.2.8** Организация (организации) по окончании назначения требует, чтобы вся соответствующая информация (включая ту, которой назначенная сторона поделилась с другими членами своей команды поставки) была поставлена, надежно сохранена, удалена или уничтожена в соответствии с корпоративными требованиями к информации и требованиями, связанными с назначением.

**9.2.9** В соответствующих случаях организация (организации) должна (должны) потребовать от назначенной стороны проверить, что определенные процедуры поставки, удаления или уничтожения конфиденциальной информации были выполнены, и проверить текущие меры безопасности для конфиденциальной информации, которая должна быть сохранена.

**9.2.10** Организация (организации) должна (должны) требовать проведения достаточных процессов вывода из операционной деятельности и демобилизации для обеспечения безопасности информации об активах.

**9.3 Реализация назначения**

**9.3.1** Организация (организации) должна контролировать и обеспечивать соблюдение всех положений, связанных с безопасностью, в документации о назначении, касающейся назначенных ею сторон, с тем чтобы они приняли приемлемый подход, ориентированный на безопасность, к выполнению своих обязательств, связанных с назначением.

**9.3.2** Организация (организации) должна (должны) сотрудничать со своей командой поставки, чтобы помочь в понимании требований по информационной безопасности и решить любые нерешенные проблемы безопасности.

**9.4 Завершение назначения**

Организация (организации) должна (должны) осуществлять надлежащие и соразмерные меры для проверки соответствия любой команды поставки любым требованиям к поставке, безопасному хранению, удалению или уничтожению конфиденциальной информации.

**Приложение А**

*(информационное)*

**Информация о контексте безопасности**

**А.1 Понимание потенциальных проблем безопасности**

Используя доступные рекомендации по безопасности, организация (организации) должна (должны) получить представление о:

a) диапазоне угроз, которые могут стремиться использовать уязвимости для:

1) компрометации ценность и долговечности инициатив и проектов;

2) компрометации ценности, долговечности и постоянного использования активов, продуктов и/или услуг организации;

3) причинения вреда, ущерба или стресса персоналу организации или другим пользователям актива или услуг, или компрометировать их;

4) нарушения или повреждения информации и/или системы;

5) нанесения ущерба репутации; и/или

6) приобретении персональных данных, интеллектуальной собственности или конфиденциальной коммерческой информации.

Примечания:

1. Угрозы включают терроризм, враждебные действия стран, коммерческий шпионаж, организованную преступность, активистов, одиночек, хакеров и злонамеренных инсайдеров.

b) спектре традиционных и развивающихся методов разведки враждебной стороны, к которым могут быть уязвимы инициативы, проекты, активы, продукты, услуги и персональная информация;

2. Во время разведки враждебная сторона ищет информацию:

1) о безопасности, которую можно экспортировать (например, физические уязвимости или конфигурация системы);

2) для определения способа действия;

3) о состоянии безопасности (т. е. о шансах быть обнаруженным /шансах на успех);

4) об образе жизни отдельного лица, группы лиц или образе использования актива.

3. С точки зрения враждебной стороны, успешное планирование атаки зависит от надежности этой информации и способности использовать ее до того, как могут быть реализованы превентивные меры.

c) возможности того, что компоненты или отдельные активы или продукты, которые будут встроены в более крупный актив, продукт или систему, будут поддельными, злонамеренно или мошеннически некачественными или искаженными;

d) потенциале и потенциальном воздействии вредоносных действий, вызванных целым рядом внешних и внутренних угроз, включая вредоносные программы, хакеров или недовольный персонал, которые могут поставить под угрозу:

1) интеллектуальную собственность и/или коммерческую конфиденциальную информацию;

2) персональную информацию;

3) целостность метаданных; или

4) целостность основных ссылочных данных.

4. Злонамеренные действия могут привести к потере, раскрытию или повреждению, несанкционированному доступу или несанкционированным изменениям информации.

e) потенциале небезопасных или плохо обслуживаемых систем для раскрытия или разрешения несанкционированного доступа к конфиденциальной информации;

f) потенциале информации, которая может быть использована для проведения анализа образа жизни с целью содействия злонамеренной или преступной эксплуатации привычек, рутины и предпочтений;

g) потенциал агрегирования информации для:

1) ведения идентификации отдельных лиц или групп лиц;

2) раскрытия конфиденциальной информации об инициативах, проектах, активах, продуктах, услугах, отдельных лицах или сообществах; или

3) раскрытия информации о конфигурации активов, продуктов, компонентов и/или программного обеспечения в системе.

5. Риски агрегирования могут возникать из-за:

1) агрегирования путем накопления, когда объем информации, хранящейся вместе, увеличивает уровень воздействия, которое могло бы произойти, если бы информация была скомпрометирована;

2) агрегирования путем ассоциации, когда объединение различных типов информации, которые сами по себе оказывают незначительное влияние или не оказывают никакого влияния при компрометации, оказывают более высокий уровень воздействия при объединении; или

3) сочетания накопления и ассоциации.

h) репутационных рисках, возникающих в связи с перечисленными выше проблемами.

**A.2 Рекомендации по безопасности**

**A.2.1** Для оказания помощи в разработке подхода, ориентированного на безопасность, организации (организациям) следует использовать соответствующие рекомендации по безопасности, чтобы получить рекомендации по рискам безопасности, возникающим в результате повышения доступности информации, интеграции услуг и систем и усиления зависимости от систем, основанных на технологиях.

**A.2.2** Если организация (организации) уже заботится о безопасности, на определенные должности в ней могут быть назначены специалисты, обладающие соответствующей квалификацией и опытом, с достаточным пониманием управления, физической, технологической, кадровой и личной безопасности, а также отношений и намерений между ними, которые могут предоставить исчерпывающие консультации и помощь в понимании контекста безопасности. В тех случаях, когда это не так, следует обратиться за консультацией к внешнему специалисту по вопросам безопасности.

**Приложение В**

*(информационное)*

**Информация о типах персонала, физических и технических средствах контроля безопасности и управления информационной безопасностью**

**В.1 Аспекты, касающиеся персонала**

При разработке политики и процессов, касающихся безопасности персонала, организациям следует учитывать, в том числе:

a) определение функций высокого риска в организации (организациях) и любых организациях, нанятых в рамках назначения или предоставления услуг;

Примечание – Примеры функций высокого риска включают функции, которые имеют доступ к деталям стратегии безопасности, информации, касающейся конфиденциальных активов, или функции по администрированию ИТ-системы или управлению ключевой информацией.

b) требования к скринингу и контрольному просмотру безопасности для любого лица (лиц), контактирующего с конфиденциальными активами, включая информацию, как в целом, так и в конкретных ролях;

c) требования к компетентности в области безопасности для лиц, выполняющих конкретные роли;

d) ознакомление всех новых сотрудников и организаций, предоставляющих услуги организации (организациям), с тем чтобы они были надлежащим образом проинформированы об их обязанностях и требуемой культуре обеспечения безопасности, включая:

1) необходимость проведения и регистрации общего обучения по вопросам безопасности в рамках проекта или текущих операций, наряду со здоровьем и безопасностью, ознакомлением с проектом или месторасположением, и другим аналогичным обучением;

2) обязательные темы, которые должны быть затронуты на этих информационных сессиях, и требуемые результаты обучения от каждого;

e) общие требования к осведомленности и подготовке в области безопасности для развития и поощрения культуры, ориентированной на безопасность, включая переподготовку;

f) требования к обучению безопасности на основе ролей для содействия принятию и поддержанию культуры, ориентированной на безопасность;

g) постоянное обучение по вопросам безопасности и требования к осведомленности;

h) требования к доступу и разрешениям по доступу к информации и информационным моделям; и

i) демобилизацию организации (организаций) и персонала.

**B.2 Физические аспекты**

При разработке политики и процессов, связанных с физической безопасностью, организации (организациям) следует учитывать, в том числе:

a) меры физической безопасности, необходимые в местах хранения конфиденциальной информации или предоставления удаленного доступа к системам в любой части конфиденциального актива;

b) меры физической безопасности (там, где это применимо), необходимые в месте расположения нового или существующего построенного объекта;

c) защиту соседних построенных объектов (там, где это применимо), которые в противном случае могут стать не видны и/или недоступны; и

Примечание – Соседние построенные активы – это построенные активы (и услуги, которые они предоставляют), которые имеют общую границу (в том числе под ними или накладные расходы) с рассматриваемым построенным активом, или находятся по соседству с этим построенным активом, построенным физически, отделенным публичной или частной улицей, публичным или частным открытым пространством или аналогичной функцией.

d) защитные меры, необходимые для вычислительных, электронных устройств и оборудования.

**B.3 Технологические аспекты**

**B.3.1** При разработке политик и процессов, связанных с технологической безопасностью, организации (организациям) следует учитывать, в том числе:

a) меры, связанные с кибербезопасностью систем сбора, обработки и хранения конфиденциальной информации, включая требование регулярной оценки уязвимости и тестирования на проникновение;

b) безопасность взаимосвязей и взаимодействий между такими системами;

c) безопасность вокруг систем, контролирующих физические активы;

d) допустимую совместимость систем и устойчивость каждой системы к сбоям;

e) процессы и процедуры управления конфигурацией и контроля изменений для систем, обрабатывающих и хранящих информацию о проектах и активах, а также техническую среду, в которой они размещаются;

f) безопасное удаление и/или уничтожение информации, хранящейся организациями, которые больше не участвуют в инициативе, проекте, активе, продукте или услуге, и/или приостановлении доступа к этой информации; и

g) если информация хранится в течение периода, необходимого для соблюдения правовых, нормативных или корпоративных требований (в зависимости от того, какой срок дольше), меры, которые должны быть применены в отношении безопасности этой сохраненной информации, и меры, которые должны быть применены после этого периода для обеспечения ее безопасного удаления, уничтожения и/или приостановления доступа.

**B.3.2** Везде, где это возможно, системы, используемые для сбора, обработки и/или хранения конфиденциальной информации, должны быть защищены по умолчанию (т. е. полная функциональность доступна без ущерба для безопасности, и настройки безопасности по умолчанию будут на самом высоком уровне) или системные настройки, настроенные для максимальной защиты этой информации.

**B.3.3** В рамках процесса отбора программные системы, используемые для сбора, обработки или хранения конфиденциальной информации, должны быть оценены на предмет их способности обеспечивать каждый из перечисленных ниже аспектов на уровне, соответствующем и пропорциональном конфиденциальности этой информации:

a) конфиденциальность – контроль и предотвращение несанкционированного доступа к информации, которая может быть конфиденциальной или нарушать конфиденциальность, отдельно или в совокупности;

b) доступность (включая надежность) – обеспечение того, чтобы информация, системы и связанные с ними процессы были постоянно под рукой, доступны, пригодны для использования и, при необходимости, раскрывались надлежащим и своевременным образом;

Примечание – Назначение может указывать доступность в процентах (например, 99 999 9 % в год) с указанным максимальным временем для восстановления нормальной работы (например, 30 минут) и может варьироваться в зависимости от активов/продуктов и услуг.

c) защищенность – системы и связанные с ними процессы разрабатываются, внедряются, эксплуатируются и поддерживаются таким образом, чтобы предотвратить создание вредоносных состояний, которые могут привести к травмам или гибели людей, непреднамеренному ущербу окружающей среде или повреждению активов;

d) устойчивость – способность информации, услуг и систем своевременно преобразовываться, обновляться и восстанавливаться в ответ на неблагоприятные события;

e) владение – системы и связанные с ними процессы разрабатываются, внедряются, эксплуатируются и поддерживаются таким образом, чтобы предотвратить несанкционированный контроль, манипуляции или вмешательство, а также гарантировать, что информация используется только в соответствии с условиями соблюдения и правами и обязанностями, указанными в документации о назначении;

f) подлинность – обеспечение того, чтобы информация, вводимая в системы и выводимая из них, состояние системы и любые связанные с ней процессы, и информация были подлинными;

g) полезность – обеспечение того, чтобы информация об активах и системах оставалась полезной в течение периода, когда может потребоваться доступ к этой информации; и

h) целостность – поддержание полноты, точности, последовательности, согласованности и конфигурации информации и систем.

**B.3.4** До внедрения любой системы, основанной на Интернете вещей или других распределенных технологиях, организации (организациям) следует:

a) понять архитектуру безопасности предлагаемых технологий;

b) определить, в какой степени архитектура соответствует требованиям безопасности организации (организаций);

c) оценить любые риски для безопасности, включая потенциальные последствия сбоя технологии, с учетом склонности организации (организаций) к риску и ожидаемых выгод, которые она может получить; и

d) принять надлежащие и соразмерные меры по снижению рисков безопасности для управления любыми неприемлемыми рисками безопасности.

**B.4 Информационная безопасность**

**B.4.1** При разработке политики и процессов, связанных с технологической безопасностью, организации (организациям) следует учитывать, в том числе:

a) требования к проведению инспекций и обследований, которые могут собирать конфиденциальную информацию, в противном случае недоступную для общественности;

b) управление и мониторинг безопасного хранения, безопасного доступа и, в конечном счете, безопасного удаления и уничтожения информации, включая информацию, которая хранится в течение определенного периода в соответствии с правовыми или иными нормативными требованиями и любыми конкретными требованиями организации (организаций), в зависимости от того, что дольше;

Приложения:

1. Важно, чтобы доступ к конфиденциальной информации осуществлялся на основе необходимых знаний, при этом организации и персонал имели доступ только к конфиденциальной информации, которая актуальна и необходима для выполнения их задач.

c) максимальный объем информации, относящейся к конфиденциальным активам/продуктам или системам, который должен содержаться в базах данных, при обменах информацией и, где это применимо, информационных моделях.

d) внедрение любых требований, касающихся какой-либо специальной обработки или защиты информации, которая имеет важное значение для безопасности и была предоставлена организации (организациям) третьей стороной;

e) защита от потери, раскрытия, повреждения или потери доступа к информации, или несанкционированных изменений информации, метаданных и справочных основных данных; и

2. Справочные основные данные содержат набор допустимых значений, которые будут использоваться другими полями данных в информационных моделях, находящихся в общем доступе.

f) мониторинг и регистрация изменений в процессах и технологиях, используемых для сбора, обработки, включая синтез и хранение информации.

**B.4.2** Политики и процессы должны применяться в течение всего жизненного цикла общей информации, что ставит под угрозу:

a) захват – действие, связанное с созданием и первоначальным хранением части информации, включая ее метаданные;

b) приобретение – покупка или передача информации от других сторон;

c) техническое обслуживание – действия, которые служат для предоставления информации, готовой к обобщению или использованию, в форме и способом, подходящими для этих целей, и включают: валидацию и верификацию; очистку; переформатирование; обогащение; перемещение; интеграцию из нескольких систем; и обновление опубликованной информации;

d) синтез – создание производной информации;

e) использование – применение информации к деятельности, функциям или задачам;

f) архивирование – копирование или размещение информации в архиве, где она хранится, но где не происходит обслуживания, использования или публикации;

g) публикация – процесс предоставления информации в организации или за ее пределами; и

h) чистка – удаление каждой известной копии отдельной части информации из организации.

**Приложение С**

*(информационное)*

**Оценка, касающаяся предоставления информации третьим сторонам**

**С.1 Оценка информации**

**C.1.1** Оценка должна включать установление:

a) того, кто будет иметь доступ к информации, которой делятся;

b) следует ли консультироваться с другими сторонами и заинтересованными сторонами до совместного использования информации и/или публикации;

c) обоснования совместного использования, в частности:

1) цель;

2) потенциальные выгоды и то, как они будут получены;

3) риски, если информация не будет передана или опубликована;

4) демонстрацию того, что предлагаемое совместное использование пропорционально цели и потенциальным выгодам; и

5) того, может ли быть достигнута цель или получены выгоды без ее совместного использования или публикации;

d) полномочий на совместное использование или публикацию информации, в частности:

1) является ли организация, которая будет осуществлять совместное использование или публиковать эту информацию, контролером информации и/или имеет право, юридические права и полномочия для этого;

2) существуют ли какие-либо юридические обязательства по распространению или публикации (например, законодательство или постановление суда); и

3) была ли она предоставлена конфиденциально.

e) любых проблем с защитой информации;

f) рисков безопасности, связанных с совместным использованием или публикацией, и того превышают ли эти риски склонность организации (организаций) к риску;

g) надлежащих и соразмерных мер по снижению рисков безопасности для решения любых проблем с защитой информации или неприемлемых рисков безопасности;

h) готовности и способности стороны, получающей информацию, надлежащим образом управлять ею; и

i) любых остаточных рисков безопасности и оставшихся проблем с защитой информации.

**C.1.2** В тех случаях, когда выявляются потенциальные нарушения/инциденты безопасности персональной информации или риски безопасности, недопустимые для организации (организаций), совместное использование или публикация должны быть запрещены до тех пор, пока не будут приняты надлежащие и соразмерные меры для устранения конфиденциальности или снижения связанных с этим рисков до уровня, приемлемого для организации (организаций).

**C.2 Регулирующие и нормативные процессы**

**C.2.1** План управления безопасностью должен подробно описывать подход к предоставлению и обмену информацией с третьими сторонами при соблюдении регулирующих и нормативных процессов.

**C.2.2** План управления безопасностью должен требовать, чтобы конфиденциальная информация была надлежащим образом разделена и защищена. Это может включать сокращение или удаление конфиденциальной информации, касающейся конфиденциальных функций, конкретных видов использования областей в пределах построенного актива и использования защитных мер. Это может также включать предоставление неструктурированной информации в таких форматах, как печатная копия, изображения или не интерактивные форматы PDF, вместо предоставления доступа, например, к интерактивным информационным моделям.

**C.2.3** В тех случаях, когда конфиденциальная информация не может быть исключена из представления, организации (организациям) следует связаться с третьей стороной до представления информации, чтобы согласовать, какие соответствующие меры защиты могут быть приняты. В тех случаях, когда на третью сторону распространяются положения законодательства о публичном доступе или прозрачности, эти меры должны быть достаточными для управления рисками до уровня, приемлемого для организации (организаций).

**C.3 Публичный доступ к информации**

В плане управления безопасностью должен быть подробно описан подход к защите конфиденциальной информации, который должен применяться в тех случаях, когда запрос на информацию поступает организацией, на которую распространяются положения законодательства об открытом доступе или прозрачности. При этом следует учитывать влияние потенциальных проблем, возникающих в результате агрегирования.

**C.4 Публичные презентации**

В плане управления безопасностью должны быть изложены требования для утверждения любых материалов, относящихся к инициативе, проекту, активу, продукту или услуге, которые будут обсуждаться или демонстрироваться на публичных мероприятиях, размещаться в местах, доступных для общественности или других третьих сторон, или публиковаться на веб-сайтах, в технических или академических публикациях или маркетинговых материалах.

**Приложение D**

*(информационное)*

**Соглашение о совместном использовании информации**

**D.1.1** Соглашение о совместном использовании информации или его эквивалент, доступное всем соответствующим сторонам, должно быть заключено до совместного использования конфиденциальной информации и информационных моделей (где это применимо), которые могут быть использованы для нанесения ущерба инициативе, проекту, активу, продукту, услуге, отдельному лицу или группе/сообществу.

**D.1.2** Детализация соглашения подразумевает как минимум:

a) цель (цели) совместного использования;

b) потенциальных получателей или типов получателей и обстоятельства, при которых они имеют доступ;

c) тип информации, подлежащей совместному использованию;

d) качество предоставляемой информации, в частности ее достоверность, охват, точность, актуальность и удобство использования;

e) требования в отношении:

1) защиты информации, в соответствующих случаях;

2) разрешенных и запрещенных прав на использование информации;

3) каскада обязательств, содержащихся в соглашении о совместном использовании информации, через уровни разрешенных дополнительных назначений; и

4) обязательств, соответствующих требованиям плана управления нарушениями безопасности/инцидентами, уведомления владельца информации и/или контролера информации в случае любого потенциального или известного нарушения безопасности или инцидента;

f) управление пользователями;

g) обслуживание информации, включая ответ на уведомление о запросе на удаление или исправление;

h) требования по информационной безопасности;

i) механизмы хранения и/или удаления совместно используемой информации;

j) процедуры рассмотрения прав субъектов информации, включая запросы на доступ, запросы и жалобы, а также передачу между организациями, территориями и юрисдикциями;

k) мониторинг и аудит выполнения соглашения о совместном использовании информации; и

l) санкции за несоблюдение соглашения о совместном использовании информации и/или нарушение/инцидент безопасности отдельным сотрудником.

Примечание – Получение соответствующей юридической консультации будет частью составления надежного соглашения об обмене информацией.

**D.1.3** В случае фактического или потенциального нарушения/инцидента безопасности или если имеются доказательства того, что информация не управляется и не обрабатывается в соответствии с соглашением о совместном использовании информации, организация (организации) должна (должны) либо:

a) приостановить действие соглашения о совместном использовании информации и обмен информацией до тех пор, пока событие или проблемы не будут расследованы и не будут согласованы и реализованы любые меры по исправлению положения; или;

Примечание – В этих обстоятельствах будет важно, чтобы расследование и осуществление мер по смягчению последствий были проведены без ненужных задержек.

b) расторгнуть соглашение о совместном использовании информации и обмене информацией и, при необходимости, потребовать удаления общей информации, если проблема не может быть удовлетворительно устранена.

**D.1.4** Соглашения о совместном использовании информации должны пересматриваться с периодичностью, определенной в плане управления безопасностью, для установления эффективности совместного использования и подтверждения того, что:

a) по-прежнему существует законная цель для продолжения совместного использования информации с каждым получателем, а там, где ее нет, этот доступ был отозван;

b) качество и обслуживание информации соответствуют согласованным стандартам; и

c) меры по информационной безопасности остаются надлежащими и соразмерными, и любые нарушения или инциденты безопасности были удовлетворительно устранены.

**Библиография**

[1] ISO 14298:2013 Graphic technology – Management of security printing processes (Графические технологии – Управление процессами защищенной печати);

[2] ISO 16530–1:2017 Petroleum and natural gas industries – Well integrity – Part 1: Life cycle governance (Нефтяная и газовая промышленность – Целостность скважин – Часть 1: Управление жизненным циклом);

[3] ISO 19011:2018 Guidelines for auditing management systems (СТ РК ISO 19011–2019 Руководящие указания по аудиту систем менеджмента);

[4] ISO 19650-1:2018 Organization and digitization of information about buildings and civil engineering works, including building information modelling (BIM) – Information management using building information modelling – Part 1: Concepts and principles (Организация и оцифровка информации о строительных объектах и работах в области гражданского строительства, включая информационное моделирование строительных объектов (BIM) – Управление информацией с использованием информационного моделирования строительных объектов – Часть 1: Концепции и принципы);

[5] ISO 22300:2012 (Е) Societal Security-Terminology (СТ РК ISO 22300-2012 Безопасность социальная. Терминология);

[6] ISO/IEC 27001:2013 Information technology – Security techniques – Information security management systems – Requirements (СТ РК ISO/IEC 27001-2015 Информационная технология – Методы и средства обеспечения безопасности – Системы менеджмента информационной безопасностью – Требования);

[7] ISO 31000 Risk management – Principles and guidelines (СТ РК ИСО 31000-2010 Менеджмент риска – Принципы и руководящие указания);

[8] ISO 55000:2014 Asset management – Overview, principles and terminology (Управление активами – Обзор, принципы и термины).

**МКС 35.240.67; 91.010.01 (IDT)**

**Ключевые слова:** конфиденциальная информация, информационная безопасность, защищенность, персональная информация, интеллектуальная собственность, склонность к риску, информационная модель

**Разработчик:**

**ТОО «Научно-исследовательский институт «Алматыгенплан»**

**Директор Ш. Сыздык**

**Советник М.А. Широкова**