ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Информационная технология

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ ТРЕБОВАНИЯ

(ISO/IEC 27001:2013, MOD)

Издание официальное

Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

Предисловие

1 РАЗРАБОТАН Государственным унитарным предприятием Центр научно-технических и маркетинговых исследований - «UNICON.UZ» (ГУП «UNICON.UZ»)

2 ВНЕСЕН Техническим комитетом по стандартизации в сфере информационных технологий и коммуникаций № 7

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Узбекского агентства стандартизации, метрологии и сертификации агентство «Узстандарт» от 05.09.2016 № 05-784

4 Настоящий стандарт модифицирован по отношению к международному стандарту ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems. Requirements (ISO/IEC 27001:2013 Информационная технология. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования).

Сведения о соответствии ссылочных государственных стандартов Республики Узбекистан международным стандартам приведены в дополнительном приложении В.

Полный перечень технических отклонений с объяснением причин их внесения приведен в приложении С.

Перевод с английского языка (en).

Степень соответствия – модифицированная (MOD).

5 ВЗАМЕН O‘z DSt ISO/IEC 27001:2009

Содержание

Введение

1 Общие положения

Цель настоящего стандарта заключается в установлении требований к разработке, внедрению, эксплуатации и непрерывному улучшению системы управления информационной безопасностью (СУИБ). Внедрение СУИБ является стратегическим решением для организации. При разработке и внедрении СУИБ должны быть учтены следующие факторы: потребности, цели, требования безопасности, используемые процессы, размер и структура организации. Предполагается, что со временем все эти влияющие на СУИБ факторы будут изменяться.

СУИБ предназначается для обеспечения конфиденциальности, целостности и доступности информации посредством использования процесса управления рисками, а также для придания уверенности заинтересованным сторонам в том, что управление рисками производится соответствующим образом.

Важно, чтобы СУИБ являлась частью общей структуры управления и была интегрирована в процессы организации, а также чтобы проектирование процессов, информационных систем и средств управления выполнялось с учетом требований информационной безопасности. Предполагается, что масштаб внедренной СУИБ будет соответствовать потребностям организации.

Настоящий стандарт может использоваться как внутренними, так и внешними сторонами при определении способности организации обеспечивать информационную безопасность в соответствии с установленными в этой организации требованиями.

Порядок представления требований в настоящем стандарте не отражает их важность или последовательность их реализации. Нумерация пунктов осуществляется исключительно только для ссылок.

Обзор семейства стандартов СУИБ, а также термины и определения, используемые во всех стандартах этого семейства (в том числе в O‘z DSt ISO/IEC 27003, O‘z DSt ISO/IEC 27004, O‘z DSt ISO/IEC 27005), содержатся в стандарте O‘z DSt ISO/IEC 27000.

2 Совместимость с другими стандартами систем управления

Для обеспечения совместимости настоящего стандарта с другими стандартами систем управления в нем применена та же высокоуровневая структура, идентичные наименования разделов, идентичный текст, общие термины и базовые термины, определенные для стандартов систем управления. Все это позволяет организации согласовать свою СУИБ с другими системами управления или интегрировать ее в общую систему управления.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Ахборот технологияси
ХАВФСИЗЛИКНИ ТАЪМИНЛАШ УСУЛЛАРИ
АХБОРОТ ХАВФСИЗЛИГИНИ БОШҚАРИШ ТИЗИМЛАРИ
ТАЛАБЛАР

Информационная технология
МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
СИСТЕМЫ УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
ТРЕБОВАНИЯ

Information technology. Security techniques. Information security management systems. Requirements

Дата введения 08.09.2016

1 Область применения

Настоящий стандарт определяет требования к разработке, внедрению, эксплуатации и непрерывному улучшению СУИБ в пределах контекста организации. Настоящий стандарт также включает требования по определению и обработке рисков информационной безопасности в соответствии с потребностями организации. Требования, устанавливаемые настоящим стандартом, предназначены для применения во всех организациях, независимо от типа, размера и сферы их деятельности. Исключение любого из требований, указанных в разделах 4 – 10, не допускается, если организация заявляет о соответствии СУИБ настоящему стандарту.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

O‘z DSt ISO/IEC 27000:2014 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь

O‘z DSt ISO/IEC 27002:2016 Информационная технология. Системы управления информационной безопасностью. Требования

Издание официальное

O‘z DSt ISO/IEC 27003:2014 Информационная технология. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью

O‘z DSt ISO/IEC 27004:2014 Информационная технология. Методы обеспечения безопасности. Измерение эффективности системы управления информационной безопасностью

O‘z DSt ISO/IEC 27005:2013 Информационная технология. Методы обеспечения безопасности. Управления рисками информационной безопасности

Примечание – При пользовании настоящим стандартом необходимо проверить действие ссылочных стандартов по указателю стандартов, составленному по состоянию на 1 января текущего года и по соответствующим информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. 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 применяют термины по O‘z DSt ISO/IEC 27000

4 Контекст организации

4.1 Понимание организации и ее контекста

Организация должна определить свой контекст, то есть совокупность внешних и внутренних факторов, которые имеют важное значение для достижения ее целей и влияют на способность СУИБ достижения предполагаемой эффективности.

Внешний контекст организации может включать следующие факторы, но не ограничиваться ими:

a) социальную и культурную, политическую, правовую, регулирующую, финансовую, технологическую, экономическую, природную и рыночную среду на международном, национальном, региональном или местном уровнях;

b) основные движущие силы и направления, воздействующие на цели организации;

c) взаимосвязи с внешними заинтересованными сторонами, их ценностями и восприятием.

Внутренний контекст организации может включать следующие факторы, но не ограничиваться ими:

a) управление, организационную структуру, роли и обязанности;

b) политики, цели и стратегии, необходимые для достижения этих целей;

c) потенциальные возможности, понимаемые как ресурсы и знания (например, капитал, время, люди, процессы, системы и технологии);

d) информационные системы, информационные потоки и процессы принятия решений (как формальные, так и неформальные);

e) взаимосвязи с внутренними заинтересованными сторонами, их ценностями и восприятием;

f) организационную культуру;

g) стандарты, руководства и модели, принятые организацией;

h) форму и содержание контрактных (договорных) отношений.

4.2 Понимание потребностей и ожиданий заинтересованных сторон

Организация должна определить:

a) заинтересованные стороны, имеющие отношение к СУИБ;

b) требования заинтересованных сторон, имеющих отношение к информационной безопасности.

Примечание - Требования заинтересованных сторон могут включать в себя законодательные, нормативные требования и договорные обязательства.

4.3 Определение области действия СУИБ

Для определения области действия СУИБ организация должна определить ее границы и возможность применения.

При определении области действия СУИБ организация должна рассмотреть следующие вопросы:

a) внешние и внутренние факторы, перечисленные в 4.1;

b) требования, указанные в 4.2;

c) интерфейсы и зависимости между деятельностью, выполняемой организацией, и деятельностью, выполняемой другими организациями.

Область действия СУИБ должна быть задокументирована.

4.4 Система управления информационной безопасности

Организация должна разработать, внедрить, эксплуатировать и непрерывно улучшать СУИБ в соответствии с требованиями настоящего стандарта.

5 Руководство

5.1 Руководство и приверженность

Высшее руководство организации должно продемонстрировать умение руководить и приверженность относительно СУИБ посредством:

a) обеспечения разработки политики и целей информационной безопасности, непротиворечащих стратегическим задачам организации;

b) обеспечения интеграции требований СУИБ в процессы организации;

c) обеспечения доступности необходимых для СУИБ ресурсов;

d) информирования о важности достижения эффективности управления информационной безопасностью и соответствии требованиям СУИБ;

e) обеспечения достижения СУИБ предполагаемой эффективности;

f) поддержки и управления персоналом, способствующих повышению эффективности СУИБ;

g) содействия постоянному улучшению;

h) поддержки других соответствующих ролей руководителей с целью демонстрации ими лидерских качеств, применительно к сфере их ответственности.

5.2 Политика

Высшее руководство должно разработать политику информационной безопасности, которая:

a) соответствует целям организации;

b) включает в себя цели информационной безопасности (см. 6.2) или обеспечивает основу для определения этих целей;

c) включает в себя приверженность к удовлетворению заданных требований по информационной безопасности;

d) включает в себя приверженность к постоянному улучшению СУИБ.

Политика информационной безопасности должна быть:

a) доступна в виде документированной информации;

b) доведена до сведения персонала организации;

c) доступна всем заинтересованным сторонам (при необходимости).

5.3 Организационные роли, ответственность и полномочия

Высшее руководство должно обеспечить определение ответственности и полномочий ролей в области информационной безопасности, а также доведение этого до сведения ответственным лицам.

Высшее руководство должно определить ответственность и полномочия для:

a) обеспечения соответствия СУИБ требованиям настоящего стандарта;

b) постоянного информирования высшего руководства об эффективности СУИБ.

Примечание - Высшее руководство может распределить ответственность и

полномочия для постоянного информирования о результативности СУИБ нескольким ответственным лицам.

6 Планирование

6.1 Действия с рисками и потенциальные возможности

6.1.1 Общие требования

При планировании СУИБ организация должна учесть факторы, перечисленные в 4.1, требования, указанные в 4.2, выявить риски и потенциальные уязвимости; все это должно быть направлено на:

a) обеспечение достижения СУИБ предполагаемой эффективности;

b) предотвращение или уменьшение нежелательных инцидентов;

c) обеспечение непрерывного улучшения.

Организация должна планировать:

a) мероприятия по обработке рисков и потенциальных уязвимостей;

b) методы:

- интеграции и реализации мероприятий в процессы СУИБ;
- оценки эффективности этих мероприятий.

6.1.2 Определение рисков информационной безопасности

Организация должна определить и внедрить процесс определения рисков информационной безопасности, который:

a) устанавливает и использует критерии рисков информационной безопасности, включающие:

1) критерии принятия рисков;

2) критерии для выполнения определения рисков информационной безопасности;

b) обеспечивает получение непротиворечивых, достоверных и сравнимых результатов периодически выполняемого определения рисков информационной безопасности;

c) идентифицирует риски информационной безопасности, в том числе:

1) применяет процесс определения рисков информационной безопасности для идентификации рисков, связанных с нарушением конфиденциальности, целостности и доступности информации в пределах области действия СУИБ;

2) идентифицирует владельцев рисков;

d) выполняет анализ рисков информационной безопасности, в том числе:

1) оценивает потенциальные последствия, которые могут возникнуть в результате реализации рисков, идентифицированных в данном пункте, перечисление c) 1);

2) оценивает реальную вероятность существования рисков, идентифицированных в данном пункте, перечисление c) 1);

3) определяет уровни рисков;

e) выполняет оценку рисков информационной безопасности, в том числе:

1) сравнивает результаты анализа рисков с критериями рисков, установленными в данном пункте, перечисление a);

2) устанавливает приоритеты обработки для проанализированных рисков.

Документированная информация с описанием процессов определения рисков информационной безопасности должна храниться в организации.

6.1.3 Обработка рисков информационной безопасности

Организация должна определить и внедрить процесс обработки рисков информационной безопасности, чтобы:

a) выбрать соответствующие способы обработки рисков информационной безопасности с учетом результатов определения рисков;

b) определить все средства управления, которые необходимы для реализации выбранных способов обработки рисков информационной безопасности;

Примечание – Организации могут самостоятельно разработать необходимые средства управления или приобрести их из любого источника.

c) сравнить средства управления, определенные в перечислении b) данного пункта, со средствами управления, приведенными в приложении A, и убедиться в том, что ни одно из необходимых средств управления не было пропущено;

Примечания

1 Приложение A содержит исчерпывающий перечень целей и средств управления. Пользователи настоящего стандарта могут обращаться к приложению A, чтобы гарантировать, что ни одно из необходимых средств управления не было проигнорировано.

2 По умолчанию цели управления включены в выбранные средства управления. В приложении A приведен далеко не исчерпывающий перечень целей и средств управления, поэтому могут потребоваться дополнительные цели и средства управления.

d) разработать Заявление о применимости, которое содержит необходимые средства управления (см. 6.1.3 b) и c)) и обоснование выбора каждого средства управления независимо от того, реализовано оно или нет, а также обоснование исключений средств управления из приложения A;

e) сформулировать план обработки рисков информационной безопасности;

f) получить одобрение плана обработки рисков информационной безопасности от владельцев рисков и подтверждение принятия остаточных рисков информационной безопасности.

Документированная информация с описанием процессов обработки рисков информационной безопасности должна храниться в организации.

6.2 Цели информационной безопасности и планирование их достижения

Организация должна установить цели информационной безопасности для соответствующих функций и уровней. Цели информационной безопасности должны:

a) соответствовать политике информационной безопасности;

b) быть измеримыми (при возможности);

c) учитывать действующие требования информационной безопасности, а также результаты определения и обработки рисков;

d) быть предоставлены соответствующему персоналу для ознакомления;

e) обновляться (при необходимости).

Документированная информация с описанием целей информационной безопасности должна храниться в организации.

При планировании достижения целей информационной безопасности организация должна определить:

a) мероприятия, которые должны быть выполнены;

b) перечень необходимых ресурсов;

c) ответственных исполнителей мероприятий;

d) сроки достижения целей;

e) метод оценки результатов.

7 Обеспечение

7.1 Ресурсы

Организация должна определить и предоставить ресурсы, необходимые для разработки, внедрения, эксплуатации и непрерывного улучшения СУИБ.

7.2 Компетентность

Организация должна:

a) определить необходимую компетентность персонала организации, от которого зависит обеспечение информационной безопасности;

b) гарантировать, что этот персонал обладает необходимой компетентностью, основанной на соответствующем образовании, тренингах или опыте работы;

c) по возможности проводить мероприятия по получению персоналом необходимой компетентности и оценивать их эффективность;

d) хранить соответствующую документированную информацию, свидетельствующую о компетентности персонала.

Примечание – Проводимые мероприятия по получению персоналом необходимой компетентности могут включать, например: проведение тренингов, наставничество или ротация штатных сотрудников; прием новых компетентных специалистов либо привлечение их для работы по совместительству.

7.3 Осведомленность

Персонал организации должен быть ознакомлен с:

a) политикой информационной безопасности;

b) его вкладом в эффективность СУИБ, включая вознаграждения за повышение уровня обеспечения информационной безопасности;

c) дисциплинарными взысканиями, последующими за неисполнением требований СУИБ.

7.4 Обмен информацией

Организация должна определить необходимость обмена информацией относительно функционирования СУИБ как с внутренними, так и с внешними заинтересованными сторонами, включая:

a) вопросы, по которым следует обмениваться информацией;

b) сроки обмена информацией;

c) заинтересованные стороны, с которыми необходимо обмениваться информацией;

d) сотрудников организации, которые должны участвовать в обмене информацией;

e) процессы, посредством которых должен осуществляется обмен информацией.

7.5 Документированная информация

7.5.1 Общие требования

СУИБ организации должна включать:

a) документированную информацию, требуемую настоящим стандартом;

b) документированную информацию, определенную организацией необходимой для обеспечения эффективности СУИБ.

Примечание - Объем документированной информации СУИБ для разных организаций может быть различным в зависимости от:

1) размера организации и вида ее деятельности, процессов, продуктов и услуг;
2) сложности процессов и их взаимодействия;
3) компетентности персонала.

7.5.2 Создание и обновление

При разработке и пересмотре документированной информации организация должна обеспечить следующее:

a) идентификацию и описание (например: название, дата, автор или ссылочный номер);

b) формат (например: язык, версия программного обеспечения, рисунки) и тип носителя (например: электронный, бумажный);

c) согласование и утверждение на предмет пригодности для применения и достоверности.

7.5.3 Управление документированной информацией

Документированной информацией, необходимой для СУИБ и требуемой настоящим стандартом, следует управлять, чтобы обеспечить:

a) доступность и пригодность для использования в тех местах и в то время, где и когда она необходима;

b) соответствующую защиту (например, от нарушения конфиденциальности или целостности, неправильного использования).

Для управления документированной информацией организация должна при возможности обеспечить следующее:

a) распространение, предоставление доступа, восстановление и использование;

b) хранение и сохранность, включая сохранность удобочитаемости;

c) управление изменениями (например, управление версиями);

d) определение сроков и места хранения.

Документированная информация внешнего происхождения, определенная организацией необходимой для планирования и функционирования СУИБ, должна быть идентифицирована и должна управляться соответствующим образом.

Примечание – Предоставление доступа предполагает выдачу разрешения только на чтение документированной информации или предоставлении полномочий на внесение в нее изменений и т.д.

8 Функционирование

8.1 Оперативное планирование и контроль

Организация должна планировать, реализовать и управлять процессами, необходимыми для выполнения требований информационной безопасности и для реализации мероприятий и методов, определенных в

6.1. Организация должна реализовать также планы достижения целей информационной безопасности, определенных в 6.2.

Организация должна иметь документированную информацию в том объеме, который необходим для обеспечения уверенности в том, что запланированные процессы выполнены.

Организация должна управлять запланированными изменениями, анализировать последствия непредусмотренных изменений и, при необходимости, принимать меры для смягчения любых неблагоприятных последствий.

Организация должна обеспечить определение и контроль процессов, выполняемых сторонними организациями.

8.2 Определение рисков информационной безопасности

Организация должна выполнять определение рисков информационной безопасности в запланированные интервалы времени или в тех случаях, когда предполагаются значительные изменения или они уже произошли, с учетом критериев, установленных в 6.1.2 a).

Документированная информация с результатами определения рисков информационной безопасности должна храниться в организации.

8.3 Обработка рисков информационной безопасности

Организация должна реализовать план обработки рисков информационной безопасности.

Документированная информация с результатами обработки рисков информационной безопасности должна храниться в организации.

9 Оценка результатов деятельности

9.1 Мониторинг, измерение, анализ и оценка

Организация должна оценивать обеспечение информационной безопасности и эффективность СУИБ.

Организация должна определить:

a) объекты мониторинга и измерения, включая процессы и средства управления информационной безопасностью;

b) методы мониторинга, измерения, анализа и оценки, по мере необходимости, которые обеспечивают достоверные результаты;

Примечание - Выбранные методы производят сравнимые и воспроизводимые результаты, которые считаются достоверными.

c) сроки проведения мониторинга и измерения;

d) сотрудников организации, которые должны проводить мониторинг и измерение;

e) сроки выполнения анализа и оценки результатов мониторинга и измерения;

f) сотрудников организации, которые должны выполнять анализ и оценку полученных результатов.

Соответствующая документированная информация с результатами мониторинга и оценки должна храниться в организации в качестве доказательства.

9.2 Внутренний аудит

Организация должна проводить внутренние аудиты СУИБ в запланированные интервалы времени для получения следующей информации о том, что:

a) соответствует ли СУИБ:

- требованиям организации;
- требованиям настоящего стандарта;

b) СУИБ эффективно внедрена и эксплуатируется.

Организация должна:

a) спланировать, разработать, внедрить и выполнять программу(ы) аудита, включая периодичность проведения, методы, ответственность, требования к планированию и отчетности. Программа(ы) аудита должна учитывать значимость проверяемых процессов и результаты предшествующих аудитов;

b) определить критерии аудита и область применения каждого аудита;

c) выполнять отбор аудиторов и процедуры аудита таким образом, чтобы обеспечить объективность и беспристрастность процесса аудита;

d) обеспечить предоставление результатов аудита соответствующему руководящему лицу;

e) сохранять документированную информацию с программой(ами) аудита и результатами аудита в качестве доказательства.

9.3 Анализ со стороны руководства

Высшее руководство должно проводить анализ СУИБ организации через запланированные интервалы времени для обеспечения ее постоянной пригодности, адекватности и эффективности.

Анализ со стороны руководства должен включать следующее:

a) состояние мероприятий по результатам предыдущих анализов со стороны руководства;

b) изменения внешних и внутренних факторов, влияющих на СУИБ;

c) замечания и предложения относительно обеспечения информационной безопасности, включая следующие вопросы:

- несоответствия и корректирующие действия;

- результаты мониторинга и измерений;
- результаты аудита;
- достижение целей информационной безопасности;

d) замечания и предложения заинтересованных сторон;

e) результаты определения рисков и состояние выполнения плана обработки рисков;

f) возможности для непрерывного улучшения.

Выводы анализа со стороны руководства должны включать решения по реализации возможностей непрерывного улучшения и каких-либо потребностей изменений СУИБ.

Соответствующая документированная информация с результатами анализа со стороны руководства должна храниться в организации в качестве доказательства.

10 Улучшение

10.1 Несоответствия и корректирующие действия

При выявлении несоответствий организация должна:

a) реагировать на несоответствия и в установленном порядке:
- принять меры по их управлению и внесению изменений;
- устранить последствия;

b) оценить необходимость принятия мер по устранению причин возникновения несоответствий с целью предотвращения их повторного возникновения в этом же или в другом месте, для этого следует:
- провести анализ несоответствий;
- определить причину несоответствий;
- определить наличие подобных несоответствий или потенциальных возможностей их возникновения;

c) реализовать любые необходимые меры;

d) проанализировать эффективность всех предпринятых корректирующих действий;

e) при необходимости внести изменения в СУИБ.

Корректирующие действия должны быть адекватны последствиям выявленных несоответствий.

Организация должна хранить документированную информацию в качестве доказательства о:

- характере несоответствий и всех последующих предпринятых мерах;
- результатах всех корректирующих действий.

10.2 Постоянное улучшение

Организация должна постоянно улучшать пригодность, адекватность и эффективность СУИБ.

Приложение А
(обязательное)

Взаимосвязь целей и средств управления

Цели и средства управления, перечисленные в таблице А.1, приведены в разделах 5 – 18 O‘z DSt ISO/IEC 27002 и должны быть использованы в контексте 6.1.3.

Таблица А.1 - Цели и средства управления

А.5	**Политики информационной безопасности**	
А.5.1	**Решение вопросов управления информационной безопасностью**	
Цель:	Обеспечить решение вопросов управления и поддержки информационной безопасности в соответствии с требованиями бизнеса, законодательства и руководящих документов.	
А.5.1.1	Политики информационной безопасности	*Средство управления* Разработка, утверждение руководством, опубликование и доведение до сведения всего персонала организации и, при необходимости, сотрудников сторонних организаций политик информационной безопасности.
А.5.1.2	Пересмотр политик информационной безопасности	*Средство управления* Пересмотр политик информационной безопасности через запланированные интервалы времени или при значительных изменениях для обеспечения их адекватности, достаточности и эффективности.
А.6	**Организация обеспечения информационной безопасности**	
А.6.1	**Внутренняя организация**	
Цель:	Создать структуру управления, которая будет инициировать и управлять обеспечением информационной безопасности в организации.	
А.6.1.1	Роли и ответственность в области информационной безопасности	*Средство управления* Определение и распределение ответственности в области информационной безопасности.
А.6.1.2	Разграничение обязанностей	*Средство управления* Разграничение взаимно противоположных обязанностей и областей ответственности для уменьшения возможности несанкционированной или непреднамеренной модификации или нецелевого использования активов организации.
А.6.1.3	Связи с государственными органами	*Средство управления* Поддержание надлежащих связей с соответствующими государственными органами власти и управления.

Продолжение таблицы А.1

А.6.1.4	Связи со специальными группами по интересам	*Средство управления* Поддержание надлежащих связей со специальными группами по интересам, или профессиональными ассоциациями, участие в форумах специалистов по информационной безопасности.
А.6.1.5	Информационная безопасность при управлении проектами	*Средство управления* Обеспечение информационной безопасности при управлении проектами независимо от типа проекта.
А.6.2	**Мобильные устройства и дистанционная работа**	
Цель:	Обеспечить безопасность дистанционной (удаленной) работы и использования мобильных устройств.	
А.6.2.1	Политика использования мобильных устройств	*Средство управления* Утверждение политики и принятие дополнительных мер безопасности для управления рисками, связанными с использованием мобильных устройств.
А.6.2.2	Дистанционная работа	*Средство управления* Внедрение политики и принятие дополнительных мер безопасности для защиты получаемой, обрабатываемой и хранимой информации в местах дистанционной работы.
А.7	**Безопасность персонала**	
А.7.1	**До трудоустройства**	
Цель:	Обеспечить уверенность в том, что персонал и работающие по договору понимают свою ответственность и соответствуют тем должностям, на которые они рассматриваются.	
А.7.1.1	Подбор персонала	*Средство управления* Выполнение проверки достоверности биографий всех претендентов на трудоустройство, выполняемой в соответствии с законодательством, нормами, этикой и соразмерно требованиям бизнеса, классификации информации, подлежащей доступу, а также принимаемым рискам.
А.7.1.2	Условия трудового договора	*Средство управления* Определение в трудовых договорах с персоналом и работающих по договору их ответственности и ответственности организации в области информационной безопасности.
А.7.2	**В период трудоустройства**	
Цель:	Обеспечить уверенность в том, что персонал и работающие по договору осведомлены об их ответственности в области информационной безопасности и соблюдают политики информационной безопасности.	
А.7.2.1	Ответственность руководства	*Средство управления* Доведение до сведения персонала и работающих по договору требования руководства о необходимости относиться должным образом к безопасности в соответствии с утвержденными политиками и процедурами организации.

Продолжение таблицы А.1

А.7.2.2	Осведомленность, обучение и тренинги в области информационной безопасности	*Средство управления* Прохождение всем персоналом организации, а там, где это необходимо, и работающими по договору, соответствующего обучения, а также регулярное получение ими обновленных вариантов политик и процедур информационной безопасности, принятых в организации и относящихся к их должностным обязанностям.
А.7.2.3	Меры дисциплинарного взыскания	*Средство управления* Наличие официально оформленных мер дисциплинарного взыскания, которые заранее были доведены до сведения персонала, налагаемых на сотрудников, нарушивших политики и процедуры информационной безопасности, принятые в организации.
А.7.3	**Порядок прекращения трудового договора и перевода на другую работу**	
Цель	Защитить интересы организации при прекращении трудового договора или переводе на другую работу	
А.7.3.1	Ответственность при прекращении трудового договора или переводе на другую работу	*Средство управления* Определение и доведение до сведения персонала или работающих по договору требования о том, что ответственность в области информационной безопасности и должностных обязанностей, продолжает действовать и после прекращения трудового договора или перевода на другую работу.
А.8	**Управление активами**	
А.8.1	**Ответственность за активы**	
Цель:	Идентифицировать активы организации и определить соответствующую ответственность за их защиту.	
А.8.1.1	Инвентаризация активов	*Средство управления* Идентификация информации, других активов, связанных с информацией, и средств обработки информации, составление инвентаризационной описи этих активов и поддержание ее в актуальном состоянии.
А.8.1.2	Владение активами	*Средство управления* Назначение владельцев активам, перечисленным в инвентаризационной описи.
А.8.1.3	Допустимое использование активов	*Средство управления* Четкое определение, документирование и внедрение правил допустимого использования информации и активов, связанных со средствами обработки информации.
А.8.1.4	Возвращение активов	*Средство управления* Обязательное возвращение всех активов организации, находящихся у персонала и пользователей сторонних организаций по окончании срока действия их трудового договора, контракта или соглашения.

Продолжение таблицы А.1

А.8.2	**Классификация информации**	
Цель:	Обеспечить надлежащий уровень защиты информации в соответствии с ее важностью для организации.	
А.8.2.1	Основные принципы классификации информации	*Средство управления* Классификация информации по требованиям законодательства, а также по важности, критичности и чувствительности для предотвращения ее несанкционированного разглашения или модификации.
А.8.2.2	Маркировка информации	*Средство управления* Разработка и внедрение соответствующего набора процедур по маркировке информации в соответствии с системой классификации, принятой в организации.
А.8.2.3	Управление активами	*Средство управления* Разработка и внедрение процедур управления активами в соответствии с системой классификации, принятой в организации.
А.8.3	**Обращение с носителями информации**	
Цель:	Предотвратить несанкционированное разглашение, модификацию, удаление или уничтожение информации, хранимой на носителях информации.	
А.8.3.1	Управление съемными носителями информации	*Средство управления* Внедрение процедур по управлению съемными носителями в соответствии с системой классификации, принятой в организации.
А.8.3.2	Утилизация носителей информации	*Средство управления* Внедрение формальных процедур по надежной и безопасной утилизации носителей информации по окончании их использования.
А.8.3.3	Безопасность носителей информации при транспортировке	*Средство управления* Защита носителей, содержащих информацию, во время транспортировки от несанкционированного доступа, неправомерного использования и повреждения.
А.9	**Управление доступом**	
А.9.1	**Требования бизнеса при управлении доступом**	
Цель:	Ограничить доступ к информации и средствам обработки информации.	
А.9.1.1	Политика управления доступом	*Средство управления* Определение, документирование и пересмотр политики управления доступом на основе требований бизнеса и требований информационной безопасности.
А.9.1.2	Доступ к сетям и сетевым сервисам	*Средство управления* Предоставление непосредственного доступа пользователям к сетям и сетевым сервисам только при наличии соответствующих полномочий.

Продолжение таблицы А.1

А.9.2	**Управление доступом пользователей**	
Цель:	Обеспечить санкционированный и предотвратить несанкционированный доступ пользователей к системам и сервисам.	
А.9.2.1	Регистрация и разрегистрация пользователей	*Средство управления* Внедрение формального процесса регистрации и разрегистрации пользователей, позволяющего назначать права доступа.
А.9.2.2	Предоставление доступа пользователям	*Средство управления* Внедрение формального процесса предоставления доступа пользователям, позволяющего предоставлять или отменять права доступа ко всем системам и сервисам пользователям всех типов.
А.9.2.3	Управление привилегированными правами доступа	*Средство управления* Ограничение и контроль предоставления и использования привилегированных прав доступа.
А.9.2.4	Управление секретной аутентификационной информацией пользователей	*Средство управления* Контроль предоставления секретной информации аутентификации посредством формального процесса управления.
А.9.2.5	Пересмотр прав доступа пользователей	*Средство управления* Регулярный пересмотр прав доступа пользователей владельцами активов.
А.9.2.6	Удаление или изменение прав доступа	*Средство управления* Удаление или изменение прав доступа всего персона и пользователей сторонних организаций к информации и средствам обработки информации при прекращении или изменении трудового договора, контракта или договора на оказание услуг.
А.9.3	**Ответственность пользователей**	
Цель:	Возложить на пользователей ответственность за сохранность их информации аутентификации.	
А.9.3.1	Использование секретной информации аутентификации	*Средство управления* Требование к пользователям о соблюдении правил организации в части использования секретной информации аутентификации.
А.9.4	**Управление доступом к системе и приложениям**	
Цель:	Предотвратить несанкционированный доступ к системам и приложениям	
А.9.4.1	Ограничение доступа к информации	*Средство управления* Ограничение доступа к информации и функциям прикладных систем в соответствии с политикой управления доступом.

Продолжение таблицы А.1

А.9.4.2	Безопасные процедуры входа в систему	*Средство управления* Выполнение управления доступом к системам и приложениям посредством безопасной процедуры входа в систему в тех случаях, когда этого требует политика управления доступом.
А.9.4.3	Система управления паролями	*Средство управления* Использование интерактивных систем управления паролями, обеспечивающих качество паролей.
А.9.4.4	Использование привилегированных программных утилит	*Средство управления* Ограничение и строгий контроль использования программных утилит (служебных программ), способных обходить системные и прикладные средства управления.
А.9.4.5	Управление доступом к исходным кодам программ	*Средство управления* Ограничение доступа к исходным кодам программ.
А.10	**Криптография**	
А.10.1	**Средства криптографической защиты информации**	
Цель:	Обеспечить правильное и эффективное использование средств криптографической защиты информации для защиты конфиденциальности, аутентичности и/или целостности информации.	
А.10.1.1	Политика использования средств криптографической защиты информации	*Средство управления* Разработка и внедрение политики использования средств криптографической защиты информации.
А.10.1.2	Управление ключами	*Средство управления* Разработка политики использования, защиты и жизненного цикла криптографических ключей и ее реализация в течение всего их жизненного цикла.
А.11	**Физическая безопасность и безопасность окружающей среды**	
А.11.1	**Охраняемые зоны**	
Цель:	Предотвратить несанкционированный физический доступ на территорию организации, повреждение информации и средств обработки информации, а также другие воздействия на них.	
А.11.1.1	Физический периметр безопасности	*Средство управления* Определение и использование периметров безопасности для защиты зон, в которых содержится чувствительная или критичная информация и средства обработки информации.
А.11.1.2	Средства управления физическим доступом	*Средство управления* Защита охраняемых зон с помощью соответствующих средств управления доступом, позволяющих обеспечивать доступ только авторизованному персоналу, который имеет соответствующие полномочия.

Продолжение таблицы А.1

А.11.1.3	Безопасность зданий, производственных помещений и оборудования	*Средство управления* Разработка и внедрение физической защиты для зданий, производственных помещений и оборудования.
А.11.1.4	Защита от внешних угроз и угроз окружающей среды	*Средство управления* Разработка и внедрение физической защиты от стихийных бедствий, злонамеренных воздействий или чрезвычайных ситуаций.
А.11.1.5	Выполнение работ в охраняемых зонах	*Средство управления* Разработка и внедрение процедур работы в охраняемых зонах.
А.11.1.6	Изолирование зон приемки и отгрузки материальных ценностей	*Средство управления* Контроль зон приемки и отгрузки материальных ценностей, а также других мест, из которых можно проникнуть в помещения, и, при возможности, изолирование их от средств обработки информации во избежание несанкционированного доступа.
А.11.2	**Безопасность оборудования**	
Цель:	Предотвратить утрату, повреждение, хищение или компрометацию активов и нарушение непрерывного функционирования организации.	
А.11.2.1	Размещение и защита оборудования	*Средство управления* Размещение и защита оборудования таким образом, который позволит снизить риски, связанные с угрозами окружающей среды и стихийными бедствиями, а также с возможностью несанкционированного доступа.
А.11.2.2	Оборудование вспомогательных служб	*Средство управления* Защита оборудования от перебоев в подаче электроэнергии и других нарушений, вызванных авариями оборудования вспомогательных служб.
А.11.2.3	Безопасность кабелей	*Средство управления* Защита силовых кабелей и кабелей телекоммуникаций, по которым передаются данные или предоставляются дополнительные информационные сервисы, от перехвата информации, взаимных помех или повреждения.
А.11.2.4	Техническое обслуживание оборудования	*Средство управления* Проведение надлежащего технического обслуживания оборудования для обеспечения его постоянной готовности и целостности.
А.11.2.5	Вынос активов	*Средство управления* Вынос оборудования, носителей с информацией или программным обеспечением из помещений организации только при наличии соответствующего разрешения.

Продолжение таблицы А.1

А.11.2.6	Безопасность оборудования и активов за пределами организации	*Средство управления* Обеспечение безопасности активов, находящихся за пределами организации, с учетом различных рисков, связанных с работой вне организации.
А.11.2.7	Безопасная утилизация или повторное использование оборудования	*Средство управления* Проверка и получение уверенности в том, что все чувствительные данные и лицензионное программное обеспечение были удалены или надежно перезаписаны до утилизации каждой единицы оборудования, содержащей запоминающие устройства.
А.11.2.8	Оборудование, оставленное пользователями без присмотра	*Средство управления* Обеспечение пользователями соответствующей защиты оборудования, оставленного без присмотра.
А.11.2.9	Политика «чистого стола» и «чистого экрана»	*Средство управления* Принятие политики «чистого стола» для бумажных документов и съемных запоминающих устройств, а также политики «чистого экрана» для средств обработки информации.
А.12	**Безопасность функционирования**	
А.12.1	**Операционные процедуры и ответственность**	
Цель:	Обеспечить надлежащее и безопасное функционирование средств обработки информации.	
А.12.1.1	Документирование операционных процедур	*Средство управления* Документирование операционных процедур и предоставление их всем пользователям, которым они необходимы.
А.12.1.2	Управление изменениями	*Средство управления* Управление изменениями в организации, бизнес-процессах, средствах и системах обработки информации, которые влияют на информационную безопасность.
А.12.1.3	Управление мощностями	*Средство управления* Мониторинг использования ресурсов, их оптимизация в соответствие с потребностями бизнеса, а также прогнозирование будущих потребностей в мощностях, обеспечивающих необходимую производительность системы.
А.12.1.4	Разделение сред разработки, тестирования и эксплуатации	*Средство управления* Разделение сред разработки, тестирования и эксплуатации, чтобы снизить риск несанкционированного доступа или внесения изменений в среду эксплуатации.

Продолжение таблицы А.1

А.12.2	**Защита от вредоносных программ**	
Цель:	Обеспечить защиту информации и средств обработки информации от вредоносных программ.	
А.12.2.1	Средства управления защитой от вредоносных программ	*Средство управления* Внедрение средств управления защитой от вредоносных программ, обеспечивающих их обнаружение и блокирование, восстановление исходного состояния, а также предназначенных для информирования пользователей.
А.12.3	**Резервное копирование**	
Цель:	Защитить от потери данных.	
А.12.3.1	Резервное копирование информации	*Средство управления* Регулярное создание и тестирование резервных копий информации, программного обеспечения и образов системы в соответствии с установленной политикой резервного копирования.
А.12.4	**Регистрация и мониторинг**	
Цель:	Фиксировать события и предоставлять свидетельства.	
А.12.4.1	Регистрация событий	*Средство управления* Создание, хранение и регулярный просмотр журналов, предназначенных для регистрации действий пользователей, исключительных ситуаций, сбоев и событий, связанных с информационной безопасностью.
А.12.4.2	Защита информации журналов регистрации	*Средство управления* Защита средств регистрации событий и информации журналов регистрации от несанкционированного вмешательства и несанкционированного доступа.
А.12.4.3	Журналы регистрации действий администратора и оператора	*Средство управления* Регистрация действий системного администратора и системного оператора, а также защита и регулярная проверка журналов регистрации их действий.
А.12.4.4	Синхронизация часов	*Средство управления* Синхронизация часов всех важных систем обработки информации внутри организации или домена безопасности с соответствующим источником сигналов точного времени.
А.12.5	**Управление эксплуатируемым программным обеспечением**	
Цель:	Обеспечить целостность эксплуатируемых систем	
А.12.5.1	Установка программного обеспечения в эксплуатируемые системы	*Средство управления* Внедрение процедур управления установкой программного обеспечения в эксплуатируемые системы.

Продолжение таблицы А.1

А.12.6	**Управление техническими уязвимостями**	
Цель:	Предотвратить использование технических уязвимостей	
А.12.6.1	Управление техническими уязвимостями	*Средство управления* Своевременное получение информации о технических уязвимостях информационных систем, оценка подверженности организации подобным уязвимостям и принятие надлежащих мер для реагирования на связанный с этими уязвимостями риск.
А.12.6.2	Ограничения на установку программного обеспечения	*Средство управления* Разработка и внедрение правил установки программного обеспечения пользователями.
А.12.7	**Аудит информационных систем**	
Цель:	Минимизировать влияние аудиторской деятельности на эксплуатируемые системы	
А.12.7.1	Средства управления аудитом информационных систем	*Средство управления* Тщательное планирование и согласование требований к аудиту и аудиторской деятельности, связанных с выполнением проверок на эксплуатируемых системах для сведения к минимуму риска нарушения бизнес-процессов.
А.13	**Безопасность обмена информацией**	
А.13.1	**Управление сетевой безопасностью**	
Цель:	Обеспечить защиту информации в сетях и поддерживающих ее средств обработки информации.	
А.13.1.1	Средства управления сетью	*Средство управления* Обеспечение управления и контроля сетями с целью защиты информации в системах и приложениях.
А.13.1.2	Безопасность сетевых сервисов	*Средство управления* Определение и включение во все соглашения о предоставлении сетевых сервисов механизмов безопасности, уровней обслуживания и требований по управлению всеми сетевыми сервисами, независимо от того, предоставляются ли данные сервисы самой организацией или специализированной сторонней организацией.
А.13.1.3	Разделение в сетях	*Средство управления* Разделение в сетях различных групп информационных сервисов и систем, а также пользователей.
А.13.2	**Передача информации**	
Цель:	Поддерживать безопасность информации, передаваемой как внутри организации, так и за ее пределы любым сторонним организациям.	
А.13.2.1	Политика и процедуры передачи информации	*Средство управления* Разработка соответствующей формальной политики, а также процедур и средств управления для защиты передачи информации с помощью всех видов средств телекоммуникаций.

Продолжение таблицы А.1

А.13.2.2	Соглашения о передаче информации	*Средство управления* Заключение соглашений о безопасной передаче бизнес-информации между организацией и сторонними организациями.
А.13.2.3	Электронный обмен сообщениями	*Средство управления* Соответствующая защита информации, содержащейся в электронных сообщениях.
А.13.2.4	Соглашения о соблюдении конфиденциальности или неразглашении информации	*Средство управления* Определение, периодический пересмотр и документирование требований, отражающих потребность организации в защите информации, для соглашений о соблюдении конфиденциальности или неразглашении информации.
А.14	**Приобретение, разработка и обслуживание информационных систем**	
А.14.1	**Требования по безопасности информационных систем**	
Цель:	Обеспечить, чтобы информационная безопасность стала неотъемлемой частью информационных систем в течение всего их жизненного цикла, а также установить требования к информационным системам, которые предоставляют сервисы по общедоступным сетям.	
А.14.1.1	Анализ и спецификация требований информационной безопасности	*Средство управления* Включение требований информационной безопасности в требования к новым или модернизируемым существующим информационным системам.
А.14.1.2	Безопасность сервисов приложений в общедоступных сетях	*Средство управления* Защита информации сервисов приложений, передаваемой по общедоступным сетям, от мошеннической деятельности, споров по контрактам, а также от несанкционированного раскрытия и модификации.
А.14.1.3	Защита транзакций сервисов приложений	*Средство управления* Защита информации, задействованной в транзакциях сервисов приложений, для предотвращения незавершенной передачи данных, ошибочной маршрутизации, несанкционированного изменения сообщений, несанкционированного раскрытия информации, несанкционированного дублирования или повторной передачи.
А.14.2	**Безопасность процессов разработки и поддержки**	
Цель:	Обеспечить разработку и внедрение информационной безопасности в течение всего жизненного цикла разработки информационных систем.	
А.14.2.1	Политика безопасной разработки	*Средство управления* Установление и применение правил по разработке программного обеспечения и систем, выполняемой организацией.
А.14.2.2	Процедуры управления изменениями системы	*Средство управления* Управление изменениями, вносимыми в системы в течение жизненного цикла их разработки, посредством использования формальных процедур управления изменениями.

Продолжение таблицы А.1

А.14.2.3	Технический анализ приложений после изменений операционных платформ	*Средство управления* Проведение анализа и тестирования критических бизнес-приложений при изменениях операционных платформ для обеспечения уверенности в том, что не будет оказано никакого отрицательного влияния на деятельность или безопасность организации.
А.14.2.4	Ограничения на внесение изменений в пакеты программ	*Средство управления* Ограничение модификаций пакетов программ только внесением необходимых изменений. Строгий контроль за всеми изменениями.
А.14.2.5	Принципы разработки безопасных систем	*Средство управления* Установление, документирование, поддержка и применение принципов разработки безопасных (защищенных) систем при внедрении любых информационных систем.
А.14.2.6	Безопасная среда разработки	*Средство управления* Установление и соответствующая защита организациями безопасных сред разработки систем и работ по их интеграции, которые охватывают весь жизненный цикл разработки системы.
А.14.2.7	Разработка системы сторонней организацией	*Средство управления* Осуществление организацией надзора и мониторинга деятельности по разработке системы, выполняемой сторонней организацией.
А.14.2.8	Тестирование безопасности системы	*Средство управления* Выполнение тестирования функциональных возможностей безопасности в процессе разработки.
А.14.2.9	Приемо-сдаточное тестирование системы	*Средство управления* Разработка программ приемо-сдаточного тестирования для новых и модернизированных систем, а также для новых версий программного обеспечения и определение соответствующих критериев.
А.14.3	**Тестовые данные**	
Цель:	Обеспечить защиту данных, используемых для тестирования.	
А.14.3.1	Защита тестовых данных	*Средство управления* Тщательный выбор, защита и контроль тестовых данных.
А.15	**Взаимоотношения с поставщиками**	
А.15.1	**Информационная безопасность при взаимоотношении с поставщиками**	
Цель:	Обеспечить защиту активов организации, к которым имеют доступ поставщики.	
А.15.1.1	Политика информационной безопасности в области взаимоотношений с поставщиками	*Средство управления* Согласование с поставщиками и документирование требований информационной безопасности, позволяющих минимизировать риски, связанные с доступом поставщиков к активам организации.

Продолжение таблицы А.1

А.15.1.2	Соглашения с поставщиками по информационной безопасности	*Средство управления* Установление всех надлежащих требований информационной безопасности и согласование их с каждым поставщиком, который может иметь доступ к информации организации и процессам управления данными, хранить и передавать информацию или поставлять компоненты инфраструктуры ИТ для организации.
А.15.1.3	Цепочки поставок информационно-коммуникационных технологий	*Средство управления* Включение в соглашения с поставщиками требований по учету рисков информационной безопасности, связанных с цепочками поставок сервисов и продуктов информационно-коммуникационных технологий.
А.15.2	**Управление сервисами, предоставляемыми поставщиками**	
Цель:	Поддерживать уровни информационной безопасности и предоставляемых сервисов, установленные в соглашениях с поставщиками.	
А.15.2.1	Мониторинг и анализ сервисов, предоставляемых поставщиками	*Средство управления* Регулярное осуществление организациями мониторинга, анализа и аудита сервисов, предоставляемых поставщиком.
А.15.2.2	Управление внесением изменений в сервисы, предоставляемые поставщиками	*Средство управления* Управление внесением изменений в предоставляемые сервисы, в том числе поддержка и совершенствование существующих политик информационной безопасности, процедур и средств управления с учетом критичности задействованных бизнес-информации, бизнес-процессов и систем, а также последующее повторное определение рисков.
А.16	**Управление инцидентами информационной безопасности**	
А.16.1	**Управление инцидентами информационной безопасности и его улучшение**	
Цель:	Обеспечить применение последовательного и эффектив-ного подхода к управлению инцидентами информационной безопасности, в том числе к обмену информацией о событиях и недостатках безопасности.	
А.16.1.1	Ответственность и процедуры	*Средство управления* Определение ответственности руководства и процедур по управлению инцидентами информационной безопасности, обеспечивающих быстрое, эффективное и организованное реагирование на эти инциденты.
А.16.1.2	Оповещение о событиях информационной безопасности	*Средство управления* Незамедлительное, насколько это возможно, оповещение руководства о событиях информационной безопасности по соответствующим каналам.

Продолжение таблицы А.1

А.16.1.3	Оповещение о недостатках информационной безопасности	*Средство управления* Предъявление требования ко всему персоналу и всем работающим по договору о необходимости отмечать и сообщать о любых наблюдаемых или предполагаемых недостатках безопасности в системах или сервисах.
А.16.1.4	Оценка событий информационной безопасности и принятие решений	*Средство управления* Оценка событий информационной безопасности и принятие решения о том, следует ли их классифицировать как инциденты информационной безопасности.
А.16.1.5	Реагирование на инциденты информационной безопасности	*Средство управления* Реагирование на инциденты информационной безопасности в соответствии с документированными процедурами.
А.16.1.6	Изучение инцидентов информационной безопасности	*Средство управления* Использование знаний, полученных при выполнении анализа и устранении инцидентов информационной безопасности, для уменьшения вероятности возникновения или влияния будущих инцидентов.
А.16.1.7	Сбор свидетельств	*Средство управления* Определение и применение процедур идентификации, сбора, получения и хранения информации, которая может служить в качестве свидетельства.
А.17	**Аспекты информационной безопасности при управлении непрерывностью бизнеса**	
А.17.1	**Непрерывность информационной безопасности**	
Цель:	Интегрировать непрерывность информационной безопасности в систему управления непрерывностью бизнеса организации.	
А.17.1.1	Планирование непрерывности информационной безопасности	*Средство управления* Определение организацией своих требований информационной безопасности и мероприятий по управлению непрерывностью информационной безопасности в нештатных ситуациях, например, в период кризиса или чрезвычайных ситуаций.
А.17.1.2	Внедрение непрерывности информационной безопасности	*Средство управления* Установление, документирование, внедрение и поддержка процессов, процедур и средств управления для обеспечения необходимого уровня непрерывности информационной безопасности в организации в нештатных ситуациях.
А.17.1.3	Верификация, анализ и оценка непрерывности информационной безопасности	*Средство управления* Регулярная верификация установленных и внедренных средств управления непрерывностью информационной безопасности для удостоверения в том, что они будут эффективно функционировать в период нештатных ситуаций.

Продолжение таблицы А.1

А.17.2	**Резервирование**	
Цель:	Обеспечить доступность средств обработки информации	
А.17.2.1	Доступность средств обработки информации	*Средство управления* Внедрение средств обработки информации с достаточной степенью резервирования для удовлетворения требований к доступности.
А.18	**Соответствие требованиям**	
А.18.1	**Соответствие требованиям законодательства и договоров**	
Цель:	Избежать нарушений требований законодательства, нормативно-правовых актов или договорных обязательств, относящихся к информационной безопасности и любым требованиям безопасности.	
А.18.1.1	Определение требований действующего законодательства и договоров	*Средство управления* Четкое определение, документирование и поддержка в соответствии с текущим состоянием дел всех имеющих отношение к каждой информационной системе и организации требований законодательства, нормативно-правовых актов и договоров, а также принятого в организации подхода к выполнению этих требований.
А.18.1.2	Права на интеллектуальную собственность	*Средство управления* Внедрение процедур, обеспечивающих соответствие требованиям законодательства, нормативно-правовых актов и договоров в области прав на интеллектуальную собственность, а также в области использования лицензионного программного обеспечения.
А.18.1.3	Защита документации организации	*Средство управления* Защита документации организации от утраты, повреждения, фальсификации, несанкционированного доступа и использования несанкционированных версий в соответствии с требованиями законодательства, нормативно-правовых актов, договоров и бизнеса.
А.18.1.4	Обеспечение приватности и защита персональной идентификационной информации	*Средство управления* Обеспечение приватности и защиты персональной идентификационной информации, при наличии соответствующих требований в законодательстве и нормативно-правовых актах.
А.18.1.5	Регулирование использования криптографических средств защиты информации	*Средство управления* Использование криптографических средств защиты информации в соответствии с требованиями всех соответствующих соглашений, законодательства и нормативно-правовых актов.

Окончание таблицы А.1

А.18.2	**Аудит и анализ информационной безопасности**	
Цель:	Обеспечить внедрение и функционирование информационной безопасности в соответствии с политиками и процедурами организации.	
А.18.2.1	Независимый аудит информационной безопасности	*Средство управления* Независимый аудит подхода организации к управлению информационной безопасностью и ее внедрения (т.е. целей управления, средств управления, политик, процессов и процедур информационной безопасности) через запланированные промежутки времени, или при значительных изменениях в реализации системы обеспечения информационной безопасности.
А.18.2.2	Соответствие политикам и стандартам безопасности	*Средство управления* Регулярный анализ соответствия процедур обработки информации соответствующим политикам безопасности, стандартам и любым другим требованиям безопасности, выполняемый руководителями в пределах своей области ответственности.
А.18.2.3	Анализ соответствия техническим требованиям	*Средство управления* Регулярный анализ соответствия информационных систем политикам организации и стандартам в области информационной безопасности.

Приложение В
(справочное)

Сведения о соответствии международных стандартов государственным стандартам Республики Узбекистан

Таблица В.1

Обозначение и наименование соответствующего международного стандарта	Степень соответствия	Обозначение и наименование ссылочного государственного стандарта Республики Узбекистан
ISO/IEC 27000:2014 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь	MOD	O‘z DSt ISO/IEC 27000:2014 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь
ISO/IEC 27002:2013 Информационные технологии. Методы обеспечения безопасности. Свод правил по управлению защитой информации	MOD	O‘z DSt ISO/IEC 27002:2016 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью
ISO/IEC 27003:2010 Информационная технология. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью	MOD	O‘z DSt ISO/IEC 27003:2014 Информационная технология. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью
ISO/IEC 27004:2009 Информационная технология. Методы обеспечения безопасности. Управление информационной безопасностью. Измерения	MOD	O‘z DSt ISO/IEC 27004:2014 Информационная технология. Методы обеспечения безопасности. Измерение эффективности системы управления информационной безопасностью
ISO/IEC 27005:2011 Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности	MOD	O‘z DSt ISO/IEC 27005:2013 Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности
Примечание - В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов: MOD - модифицированная.		

Приложение С
(справочное)

Технические отклонения и объяснение причин их внесения

С.1 Наименование настоящего стандарта изменено относительно наименования международного стандарта для приведения в соответствие стандартам серии O‘z DSt ISO/IEC 27000.

С.2 По всему тексту слова «этот документ» заменены на «настоящий стандарт».

С.3 Стандарт оформлен с учетом требований O‘z DSt 1.6:2003.

С.5 В стандарт включены отдельные изменения и дополнения. Перечень внесенных модификаций и объяснение причин их внесения приведены в таблице С.1.

Таблица С.1 – Перечень внесенных модификаций

Раздел	Модификация	Объяснение
Предисловие	Исключено	В связи с тем, что содержит информацию о разработке международного стандарта
Введение	Исключена ссылка на Директивы ISO/IEC. Часть 1. Консолидированные дополнения ISO	В связи с тем, что указанные Директивы в Республике Узбекистан не приняты
Пункт 4.1	Исключено примечание, вместо него приведено подробное изложение понимания организации и ее контекста	В связи с тем, что международный стандарт ISO 31000 не принят в качестве государственного стандарта Республики Узбекистан
Подпункт 6.1.3, последний абзац, примечание	Исключено	
Библиография	Библиографические ссылки [1], [2], [3], [4] исключены	Заменены государственными стандартами и перенесены в раздел «Нормативные ссылки» в соответствии с приложением В
	Библиографические ссылки [5], [6]	Исключены в связи с исключением ссылок по тексту стандарта
Приложение В	Дополнительно включены в текст стандарта	Приведены сведения о соответствии ссылочных международных стандартов государственным стандартам Республики Узбекистан

Окончание таблицы С.1

Раздел	Модификация	Объяснение
Приложение С		Содержит перечень технических отклонений и объяснение причин их внесения

УДК ОКС 35.040 Т 55

Ключевые слова: система управления информационной безопасностью, инцидент, политика информационная безопасность, управление рисками, определение и обработка рисков, цели и средства управления, управление доступом, организация.