ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Информационная технология

МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Системы управления информационной безопасностью

Обзор и словарь

(ISO/IEC 27000:2014, 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 связи, информатизации и телекоммуникационных технологий № 7

3 ПРИНЯТ постановлением Узбекского агентства стандартизации, метрологии и сертификации от 26.06.2014 № 05-554

4 Настоящий стандарт модифицирован относительно международного стандарта ISO/IEC 27000:2014 Information technology - Security techniques - Information security management systems – Overview and vocabulary (ISO/IEC 27000:2014 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь).

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

В стандарт внесены следующие редакционные изменения:

a) исключены информационные элементы «Предисловие» и «Библиография»;

b) слова «международный стандарт» заменены на «настоящий стандарт»;

c) добавлен новый раздел 2 «Нормативные ссылки», соответственно изменена нумерация последующих разделов;

d) исключены ссылки на нижеперечисленные международные стандарты и соответствующие им пункты, поскольку эти стандарты не приняты в качестве государственных стандартов Республики Узбекистан:

ISO/IEC 27007 Руководящие указания по аудиту систем управления информационной безопасностью;

ISO/IEC TR 27008 Руководство для аудиторов по средствам управления, используемых в системах управления информационной безопасностью;

ISO/IEC 27010 Руководство по управлению информационной безопасностью при коммуникациях между отраслями и между организациями;

ISO/IEC 27013 Руководство по интегрированному внедрению ISO/IEC 27001 и ISO/IEC 20000-1;

ISO/IEC 27014 Корпоративное управление информационной безопасностью;

ISO/IEC TR 27015 Руководство по управлению информационной безопасностью в сфере финансовых услуг;

ISO/IEC TR 27016 Управление информационной безопасностью. Организационная экономика;

ISO 27799 Информатизация здравоохранения. Управление информационной безопасностью в сфере здравоохранения;

e) для удобства пользователей настоящего стандарта в приложении B приведен алфавитный указатель английских эквивалентов терминов;

f) приведено новое приложение C, содержащее сведения о соответствии ссылочных государственных стандартов Республики Узбекистан международным стандартам.

Перевод с английского языка (en).

Степень соответствия – модифицированная (MOD).

5 ВВЕДЕН ВПЕРВЫЕ

Содержание

Введение

Цель стандартов в области систем управления информационной безопасностью (СУИБ) заключается в том, чтобы предоставить модель, которой необходимо руководствоваться при внедрении и эксплуатации СУИБ.

Предназначением семейства стандартов СУИБ является содействие организациям всех типов и размеров при внедрении и эксплуатации СУИБ. С помощью семейства стандартов СУИБ организации могут:

a) разработать и внедрить СУИБ, предназначенную для защиты их информационных активов, таких как, например, финансовой информации, информации, являющейся их интеллектуальной собственностью, персональных данных сотрудников или информации, переданной им клиентами или третьими сторонами;

b) подготовиться к независимой оценке их СУИБ.

Семейство стандартов СУИБ включает стандарты, в которых:

a) определены требования к СУИБ и органам, выполняющим сертификацию этих систем;

b) обеспечена непосредственная поддержка с помощью подробного руководства и/или руководящих указаний по реализации всеобъемлющего процесса создания, внедрения, эксплуатации и улучшения СУИБ;

c) приведены руководящие указания для СУИБ конкретных сфер деятельности;

d) рассмотрена оценка соответствия СУИБ.

В семейство стандартов СУИБ, как правило, входят стандарты под общим названием «Информационная технология. Методы обеспечения безопасности».

К семейству стандартов СУИБ относятся стандарты, рассматривающие средства управления, приведенные в O‘z DSt ISO/IEC 27002, в то время как стандарты, в которых рассматривается только внедрение средств управления, из этого семейства исключены.

В настоящем стандарте представлен обзор СУИБ, которые являются предметом рассмотрения семейства стандартов СУИБ, и определения соответствующих терминов.

Следует иметь в виду, что в разделе «Термины и определения» настоящего стандарта:

- содержатся термины и определения, наиболее часто используемые в семействе стандартов СУИБ;
- приведен неисчерпывающий перечень терминов и определений, используемых в семействе стандартов СУИБ;
- количество терминов, предназначенных для использования в семействе стандартов СУИБ, не ограничено.

Примечание - Пояснения относительно использования глагольных форм при формулировке требований и/или руководящих указаний в семействе стандартов СУИБ приведены в приложении А.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ УЗБЕКИСТАН

Ахборот технологияси
ХАВФСИЗЛИКНИ ТАЪМИНЛАШ УСУЛЛАРИ
Ахборот хавфсизлигини бошқариш тизимлари
Шарҳ ва луғат

Информационная технология
МЕТОДЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
Системы управления информационной безопасностью
Обзор и словарь

Information technology
Security techniques
Information security management systems
Overview and vocabulary

Дата введения 2014-07-01

1 Область применения

Настоящий стандарт содержит обзор систем управления информационной безопасностью, а также термины и определения, часто встречающиеся в семействе стандартов СУИБ.

Настоящий стандарт предназначен для использования в организациях всех типов (например, в коммерческих предприятиях, некоммерческих организациях и государственных учреждениях).

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

O‘z DSt ISO/IEC 17021:2009 Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента

O‘z DSt ISO/IEC 27001:2009 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования

O‘z DSt ISO/IEC 27002:2008 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью

Проект, окончательная редакция

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. Управление рисками информационной безопасности

O‘z DSt ISO/IEC 27006:2013 Информационная технология. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью

O‘z DSt ISO/IEC 27011:2014 Информационная технология. Методы обеспечения безопасности. Руководящие указания по управлению информационной безопасностью в организациях телекоммуникаций

Примечание - При пользовании настоящим стандартом целесообразно проверить действие ссылочных стандартов на территории Узбекистана по соответствующему 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, применятся в части, не затрагивающей эту ссылку.

3 Термины и определения

В настоящем стандарте использованы следующие термины с соответствующими определениями.

3.1 администрация (executive management)**:** Физическое лицо или группа лиц, которым *руководящий орган* (3.67) делегировал ответственность за реализацию стратегий и политик, направленных на достижение целей *организации* (3.51).

Примечание - Администрацией иногда называют высшее руководство, в состав которого могут входить генеральный директор, финансовый директор, заместитель генерального директора по информационным технологиям и другие аналогичные роли.

3.2 анализ (review)**:** Деятельность, предпринимаемая для установления пригодности, адекватности, *результативности* (3.63) рассматриваемого объекта для достижения установленных целей.

3.3 анализ риска (risk analysis)**:** Процесс изучения природы и характера *риска* (3.66) и определения *уровня риска* (3.81).

Примечания

1 Анализ риска служит основой для *оценки риска* (3.54) и принятия решения об *обработке риска* (3.46).

2 Анализ риска включает в себя количественную оценку риска.

3.4 аналитическая модель (analytical model)**:** алгоритм или формула, объединяющие одну или несколько *основных* (3.52) и/или *производных* (3.60) *мер* с соответствующими критериями принятия решения.

3.5 атака (attack)**:** Попытка уничтожить, раскрыть, изменить, заблокировать, перехватить, получить несанкционированный доступ или несанкционированно использовать активы.

3.6 атрибут (attribute)**:** Свойство или характеристика *объекта* (3.47), которые могут быть определены количественно или качественно непосредственно человеком или с помощью автоматизированных средств.

3.7 аудит (audit)**:** Систематический, независимый и документированный *процесс* (3.61) получения свидетельств аудита и их объективной оценки для определения степени выполнения согласованных критериев аудита.

Примечание - Аудит может быть внутренним (аудитом первой стороны) или внешним (аудитом второй или третьей стороны), либо комплексным (аудитом, объединяющим два или более различных аспектов).

3.8 аутентификация (authentication)**:** Обеспечение уверенности в том, что предъявленный логическим объектом идентификатор является подлинным.

3.9 аутентичность, подлинность (authenticity)**:** Свойство, гарантирующее, что логический объект идентичен заявленному.

3.10 аутсорсинг (outsource)**:** Передача *организацией* (3.51) по договору выполнения части своих функций или *процессов* (3.61) специализированной внешней организации.

Примечание – Несмотря на то, что внешняя организация находится за пределами *системы управления* (3.68) организации, выполняемые внешней организацией функции или процессы находятся в пределах этой системы управления.

3.11 валидация (validation)**:** Подтверждение посредством представления объективных свидетельств того, что требования, предназначенные для конкретного использования или применения, выполнены.

3.12 верификация (verification)**:** Подтверждение посредством представления объективных свидетельств того, что установленные требования были выполнены.

Примечание – Верификацию также можно назвать тестированием на соответствие.

3.13 вероятность (likelihood)**:** Характеристика возможности и частоты появления события.

3.14 владелец риска (risk owner)**:** Физическое лицо или логический объект, несущие ответственность и имеющие полномочия по управлению *риском* (3.66).

3.15 внешняя область применения (external context): Внешние условия, в которых организация работает и достигает своих целей.

Примечание - Внешняя область применения может включать в себя:

- внешнюю среду, связанную с культурной, социальной, политической, законодательной, регулирующей, экономической, природной или конкурентной сферой на международном, национальном, региональном или местном уровнях;
- ключевые критерии и тенденции, которые могут воздействовать на достижение установленных *целей* (3.85) *организации* (3.51);
- взаимоотношения с внешними заинтересованными сторонами, восприятие ими риска, а также значимость для организации этих *заинтересованных сторон* (3.24).

3.16 внутренняя область применения (internal context): Внутренние условия, в которых организация работает и достигает своих целей.

Примечание - Внутренняя область применения может включать в себя:

- управление, организационную структуру, обязанности и подотчетность;
- политику, цели и задачи, а также стратегию их достижения;
- возможности организации с точки зрения ресурсов и знаний (например, капитал, время, люди, процессы, системы и технологии);
- информационные системы, информационные потоки и процессы принятия решений (формальные и неформальные);
- взаимоотношения с внутренними заинтересованными сторонами, восприятие ими риска и значимость для организации этих заинтересованных сторон;
- культуру организации;
- стандарты, руководящие принципы и модели работы, принятые в организации;
- форму и объем договорных отношений.

3.17 высшее руководство (top management)**:** Физическое лицо или группа лиц, осуществляющих руководство и управление *организацией* (3.51) на высшем уровне.

Примечания

1 Высшее руководство имеет возможность делегировать полномочия и снабжать ресурсами в пределах организации.

2 Если область действия *системы управления* (3.68) распространяется только на некоторые подразделения *организации* (3.51), тогда в состав высшего руководства входят только те лица, которые осуществляют руководство и управление этими подразделениями.

3.18 данные (data)**:** Совокупность заданных величин для *основных* (3.52) и *производных мер* (3.60) и/или *индикаторов* (3.27).

Примечание – Это определение применительно только в контексте O‘z DSt ISO/IEC 27004.

3.19 доверенный центр обмена информацией (trusted information communication entity)**:** Автономная организация, обеспечивающая обмен информацией в пределах сообщества по обмену информацией.

3.20 документированная информация (documented information)**:** Информация, необходимая для управления и функционирования *организации* (3.51), а также материальный носитель, на котором она содержится.

Примечания

1 Документированная информация может быть представлена в любой форме и на любом носителе, также она может быть получена из любого источника.

2 Документированная информация может ссылаться на:

- *систему управления* (3.68), включая связанные с ней *процессы* (3.61);
- информацию, созданную для функционирования организации (документацию);
- свидетельства достижения результатов (записи).

3.21 достоверность (reliability)**:** Свойство соответствия предусмотренному поведению или результату.

3.22 доступность (availability)**:** Свойство быть доступным и пригодным к использованию по запросу авторизованного логического объекта.

3.23 единица измерения (unit of measurement)**:** Действительная скалярная величина, определенная и принятая по соглашению, с которой можно сравнить любую другую величину того же рода и выразить их отношение в виде числа.

3.24 заинтересованная сторона (interested party, stakeholder)**:** Физическое лицо или *организация* (3.51), которые могут воздействовать, подвергаться воздействию или осознавать, что на них влияет какое-либо решение или деятельность.

3.25 идентификация риска (risk identification)**:** Процесс определения, составления перечня и описания *риска* (3.66).

Примечания

1 Идентификация риска может включать в себя источники риска, события, их причины и возможные последствия.

2 Идентификация риска может также включать в себя теоретический анализ, анализ хронологических данных, экспертных оценок и потребностей заинтересованных сторон.

3.26 измерение (measurement)**:** *Процесс* (3.61) определения значения.

Примечание - В контексте *информационной безопасности* (3.28) для выполнения процесса определения значения потребуется информация о *результативности* (3.63) *системы управления* (3.68) информационной безопасностью и взаимодействующих с ней *средств управления* (3.74), используемых *методе измерения* (3.40), *функции измерения* (3.83), *аналитической модели* (3.4) и *критериях принятия решения* (3.37).

3.27 индикатор (indicator)**:** *Мера* (3.39), позволяющая оценить соответствующие *атрибуты* (3.6), полученные из *аналитической модели* (3.4), разработанной для определенных *информационных потребностей* (3.29).

3.28 информационная безопасность (information security)**:** Сохранение *конфиденциальности* (3.33), *целостности* (3.84) и *доступности* (3.22) информации.

Примечание – Можно также выделить и другие, не всегда обязательные, свойства информационной безопасности, например, *аутентичность* (3.9), подотчетность, *неотказуемость* (3.42) и *достоверность* (3.21).

3.29 информационная потребность (information need)**:** Достоверные знания, необходимые для управления целями, задачами, рисками и проблемами.

3.30 информационная система (information system)**:** Приложения, сервисы, активы информационных технологий или любые другие компоненты обработки информации.

3.31 инцидент информационной безопасности (information security incident)**:** Единичное событие или ряд нежелательных или непредвиденных *событий информационной безопасности* (3.70), из-за которых велика вероятность компрометации бизнес-операций и угрозы *информационной безопасности* (3.28).

3.32 компетентность (completence): Способность применять знания и навыки для достижения желаемых результатов.

3.33 конфиденциальность (confidentiality)**:** Свойство информации быть недоступной или закрытой для неавторизованных лиц, логических объектов или *процессов* (3.61).

3.34 корпоративное управление информационной безопасностью (governance of information security): Система, обеспечивающая руководство и контроль деятельности *организаций* (3.51) в области информационной безопасности.

3.35 корректирующее действие (corrective action)**:** Действие, предпринятое для устранения причины обнаруженного *несоответствия* (3.44) и предотвращения его повторного возникновения.

3.36 коррекция (correction): Действие, предпринятое для устранения обнаруженного *несоответствия* (3.44).

3.37 критерии принятия решений (decision criteria)**:** Пороговые и заданные величины или эталоны, используемые для определения потребности в деятельности или дальнейшем исследовании, или для описания уровня достоверности данного результата.

3.38 критерии риска (risk criteria)**:** Показатели, по которым оценивают значимость *риска* (3.66).

Примечания

1 Критерии риска основаны на установленных целях организации, внешней и внутренней среды организации.

2 Критерии риска могут быть сформированы на основе требований стандартов, политики, законодательства и иных требований.

3.39 мера (measure)**:** Переменная, значение которой присваивается в процессе *измерения* (3.26).

Примечание – Термин «меры» используется для определения совокупности базовых и производных мер, а также индикаторов.

3.40 метод измерения (measurement method)**:** Логическая последовательность операций, описанная в общем виде и используемая для измерения *атрибута* (3.6) с помощью определенной *шкалы* (3.88).

Примечание – Вид метода измерения зависит от характера операций, используемых при измерении атрибута. Различают два вида метода измерения:

- субъективный: количественная оценка включает человеческую оценку;
- объективный: количественная оценка основана на математических правилах.

3.41 мониторинг (monitoring)**:** Определение состояния системы, процесса (3.61) или деятельности.

Примечание – Для определения состояния возможно будет необходимо его контролировать, наблюдать или критически оценивать.

3.42 неотказуемость (non-repudiation)**:** Возможность доказать возникновение определенного события или действия и определить инициирующие их логические объекты.

3.43 непрерывность информационной безопасности (information security continuity)**:** *Процессы* (3.61) и процедуры, обеспечивающие непрерывность функционирования *информационной безопасности* (3.28).

3.44 несоответствие (nonconformity)**:** Невыполнение *требования* (3.76).

3.45 обмен информацией и консультации относительно риска (risk communication and consultation)**:** Непрерывные итеративные процессы, выполняемые организацией для обеспечения, распространения или получения информации и участия в диалоге с *заинтересованными сторонами* (3.24) по вопросам, относящимся к управлению *рисками* (3.66).

Примечания

1 Информация может относиться к существованию, природе, форме, вероятности, значимости, оценке, приемлемости и обработке риска.

2 Консультации являются двухсторонним процессом обмена информацией между организацией и ее заинтересованными сторонами по проблеме до принятия решения или определения действий по этой проблеме.

Консультация - это:

- процесс, который способствует принятию решения на основе убеждения, а не под давлением;

- процесс, который предшествует процессу принятия решения, но не объединяется с ним.

3.46 обработка риска (risk treatment)**:** *Процесс* (3.61) модификации *риска* (3.66).

Примечания

1 Обработка риска может включать в себя:

- исключение риска путем принятия решения не начинать или не продолжать деятельность, в процессе или в результате которой может возникнуть опасное событие;

- принятие или повышение риска для обеспечения более широких возможностей;

- устранение источников риска;

- изменение вероятности опасного события;

- изменение последствий опасного события;

- разделение риска с другой стороной или сторонами (путем включения в контракты или финансирования обработки риска);

- обоснованное решение о сохранении риска.

2 Обработка риска может включать в себя устранение, предотвращение или снижение риска.

3 При обработке риска могут возникнуть новые риски и могут измениться существующие риски.

3.47 объект (object)**:** Отдельный элемент, характеризуемый посредством *измерения* (3.26) его *атрибутов* (3.6).

3.48 объект анализа (review object)**:** Анализируемый специфический элемент.

3.49 объём аудита (audit scope)**:** Продолжительность и границы *аудита* (3.7).

3.50 определение риска (risk assessment)**:** *Процесс* (3.61), включающий *идентификацию риска* (3.25), *анализ риска* (3.3) и *оценку риска* (3.54).

3.51 организация (organization)**:** Физическое лицо или группа лиц, выполняющие определенные функции, несущие определенную ответственность, а также обладающие определенными полномочиями и взаимоотношениями, необходимыми для достижения определенных *целей* (3.85).

3.52 основная (базовая) мера (base measure)**:** *Мера* (3.39), определенная в терминах *атрибута* (3.6) и метода его количественного определения.

Примечание – Основная мера функционально независима от других мер.

3.53 остаточный риск (residual risk)**:** *Риск* (3.66), оставшийся после *обработки риска* (3.46).

Примечания

1 Остаточный риск может представлять собой неопределенный риск.

2 Остаточный риск иногда называют «сохраняемым риском».

3.54 оценка риска (risk evaluation)**:** *Процесс* (3.61) сравнения результатов *анализа риска* (3.3) с *критериями риска* (3.38) для определения *риска* (3.66) и/или приемлемости, или допустимости его величины.

Примечание - Сравнительная оценка риска может быть использована при принятии решения об *обработке риска* (3.46).

3.55 политика (policy)**:** Цели и распоряжения *организации* (3.51), формально выраженные ее *высшим руководством* (3.17).

3.56 последствие (consequence)**:** Результат воздействия *события* (3.69) на *цели* (3.85).

Примечания

1 Результатом воздействия события может быть одно или несколько последствий.

2 Последствия могут быть определенными или неопределенными, могут быть ранжированы от позитивных до негативных.

3 Последствия могут быть выражены качественно или количественно.

4 Первоначальные последствия могут вызвать эскалацию дальнейших последствий по принципу «домино».

3.57 постоянное улучшение (continual improvement)**:** Повторяющаяся деятельность по улучшению *результатов деятельности* (3.64).

3.58 принятие риска (risk acceptance)**:** Решение принять *риск* (3.66).

3.59 проект СУИБ (ISMS project)**:** Структурированные виды деятельности, предпринимаемые *организацией* (3.51) при внедрении СУИБ.

3.60 производная мера (derived measure)**:** *Мера* (3.39), которая определяется как функция двух или более значений *основных мер* (3.52).

3.61 процесс (process)**:** Совокупность взаимосвязанных и взаимодействующих видов деятельности, преобразующая входы в выходы.

3.62 процесс управления риском (risk management process)**:** Взаимосвязанные действия по обмену информацией, консультациям, установлению целей, области применения, идентификации, исследованию, оценке, обработке, мониторингу и анализу *риска* (3.66), выполняемые в соответствии с политикой, процедурами и методами управления организации.

Примечание – В O‘z DSt ISO/IEC 27005 термин «процесс» используется для полного описания управления риском. Элементы в пределах процесса управления риском называют «деятельностью».

3.63 результативность (effectiveness)**:** Степень реализации запланированной деятельности и достижения запланированных результатов.

3.64 результаты деятельности (performance)**:** Измеримый результат.

Примечание – Результаты деятельности могут быть выражены в количественных и качественных показателях.

3.65 результаты измерения (measurement results)**:** Один или более *индикаторов* (3.27) и ассоциированных с ними интерпретаций, соответствующие *информационной потребности* (3.29).

3.66 риск (risk)**:** Следствие влияния неопределенности на достижение поставленных целей.

Примечания

1 Под следствием влияния неопределенности необходимо понимать отклонение от ожидаемого результата или события (позитивное и/или негативное).

2 Неопределенность - это состояние полного или частичного отсутствия информации, необходимой для понимания *события* (3.69), его *последствий* (3.56) и их *вероятностей* (3.13).

3 Риск часто характеризуют путем описания возможного *события* (3.69) и его *последствий* (3.56) или их сочетания.

4 Риск часто представляют в виде *последствий* (3.56) возможного события (включая изменения обстоятельств) и соответствующей *вероятности* (3.13) события.

5 В контексте систем управления информационной безопасностью риски информационной безопасности могут быть представлены в виде влияния неопределенности на цели информационной безопасности.

6 Риск информационной безопасности связан с вероятностью использования *угрозами* (3.77) *уязвимостей* (3.82) информационных активов или группы информационных активов, в результате чего будет нанесен ущерб организации.

3.67 руководящий орган (governing body)**:** Физическое лицо или группа лиц, ответственных за соответствующие результаты деятельности (3.64) организации (3.51).

Примечание – Руководящим органом может быть совет директоров.

3.68 система управления (management system)**:** Совокупность взаимосвязанных или взаимодействующих элементов *организации* (3.51), на основе которых разрабатываются *политики* (3.55), *цели* (3.85) и *процессы* (3.61), необходимые для достижения целей организации.

Примечания

1 Система управления может контролировать одну или более сфер деятельности.

2 Элементы системы включают структуру организации, роли и ответственности, планирование, процессы и т.д.

3 Область действия системы управления может распространяться на всю организацию, специальные и общие функции организации, специальные и общие подразделения организации, или на одну или более функций, выполняемых группой организаций.

3.69 событие (event)**:** Случай определенного стечения обстоятельств.

Примечания

1 Событие может быть единичным или многократным и может иметь несколько причин.

2 Событие может быть определенным или неопределенным.

3 Вместо термина «событие» также могут быть использованы термины «инцидент» или «несчастный случай».

3.70 событие информационной безопасности (information security event)**:** Идентифицированный случай состояния системы, услуги или сети, указывающий на возможное нарушение политики безопасности или на отказ средств защиты, либо на ранее неизвестную ситуацию, которая может быть существенной для безопасности.

3.71 сообщество по обмену информацией (information sharing community)**:** Группа организаций, заключивших соглашение об обмене информацией.

Примечание - Организацией может называться и индивидуальный предприниматель.

3.72 соответствие (conformity)**:** Выполнение требования.

3.73 средства обработки информации (information processing facilities)**:** Любая система обработки информации, сервисы или инфраструктура, или места, где они физически расположены.

3.74 средства управления (controls)**:** Мера, применяя которую, модифицируют риск (3.66).

Примечания

1 К средствам управления относятся любые процессы, политики, устройства, процедуры или иные действия, направленные на модификацию риска.

2 Средства управления не всегда могут выполнять предполагаемую или допускаемую модификацию.

3.75 стандарт в области обеспечения безопасности (security implementation standard)**:** Официально принятый документ, устанавливающий методы обеспечения безопасности.

3.76 требование (requirement)**:** Потребность или ожидание, которое установлено, обычно предполагается или является обязательным.

Примечания

1 Выражение «обычно предполагается» означает, что это общепринятая практика организации и заинтересованных сторон, когда предполагаются рассматриваемые потребности или ожидания.

2 Установленным является такое требование, которое определено, например, в документированной информации.

3.77 угроза (threat)**:** Потенциальная причина нежелательного инцидента, который может причинить ущерб системе или организации.

3.78 управление доступом (access control)**:** Методы обеспечения санкционированного и ограниченного доступа к активам, основанные на требованиях бизнеса и безопасности.

3.79 управление инцидентами информационной безопасности (information security incident management)**:** *Процессы* (3.61) обнаружения, учета, оценки, реагирования и изучения, относящиеся к *инцидентам информационной безопасности* (3.31).

3.80 управление риском (risk management)**:** Скоординированная деятельность по руководству и управлению *организацией* (3.51) в области *риска* (3.66).

3.81 уровень риска (level of risk)**:** Величина *риска* (3.66), характеризуемая сочетанием *последствий* (3.56) и их *вероятности* (3.13).

3.82 уязвимость (vulnerability)**:** Слабость *активов* или *средств управления* (3.74), которая может быть использована одной или более *угроз* (3.77).

3.83 функция измерения (measurement function)**:** Алгоритм или формула, посредством которых производится объединение двух или более *основных мер* (3.52).

3.84 целостность (integrity)**:** Свойство сохранения правильности и полноты.

3.85 цель (objective)**:** Результат, который предполагается достичь.

Примечания

1 Цель может быть стратегической, тактической или оперативной.

2 Цели могут устанавливаться для разных сфер деятельности (например, для финансовой сферы, здравоохранения и безопасности, а также для показателей качества окружающей среды) и для разных уровней (например, стратегические цели организации, проекта, продукта и *процесса* (3.61).

3 Цель может быть выражена и другими способами, например, как запланированный результат, намерение, действующий критерий, как цель информационной безопасности или с помощью других слов-синонимов (например, замысел, показатель или задача).

4 В контексте систем управления информационной безопасности для достижения конкретных результатов устанавливаются цели информационной безопасности, соответствующие политике информационной безопасности организации.

3.86 цель анализа (review objective)**:** Записанное изложение полученных результатов анализа.

3.87 цель управления (control objective)**:** Описанное состояние, которое должно быть достигнуто в результате внедрения *средств управления* (3.74).

3.88 шкала (scale)**:** Непрерывное или дискретное упорядоченное множество значений или множество категорий, на которых отображается *атрибут* (3.6).

Примечание – Вид шкалы зависит от характера взаимосвязи между ее значениями. Обычно различают четыре вида шкал:

- шкала наименований (номинационная или номинальная): значения измерений - категории;
- шкала порядковая (ординальная или ранговая): значения измерений - ранги;
- шкала интервалов (интервальная): деления шкалы расположены равномерно и соответствуют одинаковым значениям атрибута;
- шкала отношений (относительная): деления шкалы расположены равномерно и соответствуют одинаковым значениям атрибута. Шкала отношений имеет фиксированный ноль, который соответствует полному отсутствию атрибута.

Приведены примеры только основных видов шкал.

4 Системы управления информационной безопасностью

4.1 Введение

Организации всех типов и размеров:

a) собирают, обрабатывают, хранят и передают большое количество информации;

b) признают, что информация и связанные с ней процессы, системы, сети и персонал являются важными активами, необходимыми для достижения целей организации;

c) сталкиваются с множеством рисков, которые могут повлиять на функционирование активов;

d) модифицируют риски путем внедрения средств управления информационной безопасностью, иначе называемых «меры безопасности» или «контрмеры».

Вся информация, хранимая и обрабатываемая организацией, является объектом, подверженным угрозам атак, появлению ошибок, воздействию

природных катаклизмов (например, наводнению или пожару) и т.п., и является изначально уязвимым объектом при его использовании. Понятие «информационная безопасность» обычно основывается на следующем: информация рассматривается в качестве актива, который имеет величину и требует соответствующей защиты, например, от нарушения доступности, конфиденциальности и целостности. Использование точной и полной информации, которая доступна в нужный момент времени по санкционированному запросу является катализатором эффективности бизнеса.

Защита информационных активов посредством определения, достижения, поддерживания и повышения эффективности информационной безопасности является существенным условием для достижения организацией ее целей, соблюдения законодательства, поддержания и повышения ее имиджа. Эта скоординированная деятельность, направленная на внедрение соответствующих средств управления и обработку неприемлемого риска информационной безопасности, общеизвестна как основа управления информационной безопасностью.

Так как риски информационной безопасности и эффективность средств управления меняются в результате изменения обстоятельств, то организации должны:

a) проверять и оценивать эффективность реализованных средств управления и процедур;

b) определять вновь появившиеся риски для последующей их обработки;

c) выбирать, внедрять и, при необходимости, совершенствовать соответствующие средства управления.

Чтобы эта деятельность в области информационной безопасности была взаимоувязана и скоординирована, каждой организации необходимо определить свои цели и политику в области информационной безопасности, а затем стремиться к достижению этих целей, эффективно используя систему управления.

4.2 Общие положения

4.2.1 Краткий обзор и принципы

В состав СУИБ, предназначением которой является защита информационных активов организации, входят политики, процедуры, руководящие указания, а также взаимосвязанные с ними ресурсы и различные виды деятельности, коллективно управляемые организацией. СУИБ представляет собой системный подход к созданию, внедрению, эксплуатации, мониторингу, анализу, техническому обслуживанию и совершенствованию информационной безопасности организаций при достижении ими своих бизнес-целей. СУИБ основывается на оценке риска и уровнях принимаемых организациями рисков и предназначена для эффективной обработки и управления рисками. Успешному внедрению

СУИБ будут содействовать анализ требований по защите информационных активов и применение соответствующих средств управления с целью обеспечения необходимой защиты этих информационных активов. Также успешному внедрению СУИБ будут содействовать следующие фундаментальные принципы:

a) осведомленность о необходимости информационной безопасности;

b) назначение ответственных за информационную безопасность;

c) объединение обязательств руководства и интересов посредников;

d) повышение социального значения;

e) определение в процессе оценки рисков необходимых средств управления для достижения приемлемого уровня рисков;

f) придание безопасности статуса необходимого элемента информационных сетей и систем;

g) активное предотвращение и обнаружение инцидентов информационной безопасности;

h) обеспечение комплексного подхода к управлению информационной безопасностью;

i) непрерывная переоценка информационной безопасности и внесение необходимых изменений.

4.2.2 Информационные активы

Информационные активы аналогично другим важным активам играют существенную роль в деятельности организации, и, следовательно, они должны быть защищены должным образом. Формы хранения информационных активов могут быть разнообразными: в том числе в цифровой форме (например, файлы данных, записанные на электронные или оптические носители), в материальной форме (например, на бумаге), а также и в нематериальной форме - в форме знаний сотрудников. Информационные активы могут передаваться различными средствами: посредством курьера, по электронной почте или по телефону. Независимо от того, в какой форме существуют информационные активы или с помощью каких средств осуществляется их передача, информационным активам всегда нужна соответствующая защита.

Информационные активы организаций зависят от информационно-коммуникационных технологий. Эти технологии часто являются существенным элементом любой организации и помогают облегчить создание, обработку, хранение, передачу, защиту и уничтожение информационных активов.

4.2.3 Информационная безопасность

Информационная безопасность имеет три основных характеристики: конфиденциальность, доступность и целостность. Обеспечение информационной безопасности подразумевает использование необходимых мер безопасности, выбираемых с учетом множества угроз, и управление этими

мерами, обеспечивая тем самым поддержку успешности и непрерывности бизнеса, а также минимизацию влияния инцидентов информационной безопасности.

Информационная безопасность обеспечивается посредством внедрения соответствующего комплекса средств управления, выбранных в процессе управления рисками. Управление информационной безопасностью осуществляет СУИБ, которая для защиты соответствующих информационных активов использует политики, процессы, процедуры, организационные структуры, программное обеспечение и аппаратные средства. Для того, чтобы удостовериться в том, что цели безопасности и бизнес-цели организации достигнуты, эти средства управления должны быть определены, внедрены, проверены, оценены и при необходимости усовершенствованы. Предполагается, что соответствующие средства управления информационной безопасностью будут полностью интегрированы в бизнес-процессы организации.

4.2.4 Управление

Управление – это деятельность соответствующих структур по политике развития, контролю и непрерывному улучшению организации. К управленческой деятельности относятся действия, способы или опыт организационной работы, регулирование, координация, контроль и управление ресурсами. Управленческая структура организации зависит от размера организации: в небольшой организации она может состоять из одного руководителя, а в больших организациях – иметь управленческую иерархию, состоящую из множества руководителей разных рангов.

Относительно СУИБ управление включает контроль и принятие решений, необходимых для достижения бизнес-целей, посредством защиты информационных активов организации. Управление информационной безопасностью заключается в формулировании и использовании политик информационной безопасности, стандартов, процедур и рекомендаций, которые будут затем применяться во всех подразделениях организации и всеми лицами, взаимодействующими с этой организацией.

4.2.5 Система управления

Система управления использует основные ресурсы для достижения целей организации. Система управления включает организационную структуру, политики, планирование деятельности, обязанности, методы, процедуры, процессы и ресурсы.

С точки зрения информационной безопасности система управления позволяет организации:

a) удовлетворять требованиям по безопасности заказчиков и других заинтересованных сторон;

b) улучшать планы организации и деятельности;

c) соответствовать целям информационной безопасности организации;

d) выполнять требования стандартов, законодательных и нормативно-правовых актов;

e) управлять информационными активами способом, который облегчает непрерывное улучшение и корректировку существующих целей организации и среды.

4.3 Процессный подход

Для эффективного функционирования организации необходимо управлять многими определенными видами деятельности. Любой вид деятельности, связанный с использованием ресурсов, который нуждается в управлении для выполнения преобразований входов в выходы с использованием при этом ряда взаимосвязанных или взаимодействующих видов деятельности, может рассматриваться как процесс. Выход одного процесса может быть непосредственно преобразован во вход другого процесса и обычно это преобразование выполняется в соответствии с запланированными и контролируемыми условиями. Использование системы процессов в пределах организации совместно с идентификацией, взаимодействием и управлением этих процессов может рассматриваться как «процессный подход».

4.4 Значимость СУИБ

Риски, связанные с информационными активами организации, должны быть учтены. Для обеспечения информационной безопасности необходимо управлять рисками и исключить риски, связанные с физическими, человеческими и технологическими факторами угроз для всех видов информации, используемых в организации.

Предполагается, что внедрение СУИБ должно стать стратегическим решением для организации; необходимо, чтобы это решение было полностью интегрировано, масштабировано и приведено в соответствии с потребностями организации.

На разработку и внедрение СУИБ организации оказывают влияние потребности и цели организации, требования безопасности, используемые бизнес-процессы, размер и структура организации. При разработке и функционировании СУИБ должны быть учтены интересы и требования информационной безопасности всех сторон, заинтересованных в деятельности организации, в том числе заказчиков, поставщиков, деловых партнеров, акционеров и других соответствующих третьих сторон.

Во взаимосвязанном мире информация и связанные с ней процессы, системы и сети составляют критические бизнес-активы. Организации, а также их информационные системы и сети сталкиваются с угрозами безопасности из множества разнообразных источников, включая компьютерное мошенничество, шпионаж, саботаж, вандализм, пожары и наводнения. Ущерб информационным системам и сетям может быть также

нанесен злонамеренными кодами, действиями компьютерных хакеров, атаками типа «отказ в обслуживании», которые становятся все более распространенными, сложными и изощренными.

СУИБ важны для предприятий как государственного, так и частного сектора. В любой отрасли производства СУИБ является инструментом, который обеспечивает поддержку электронного бизнеса, и основой деятельности в области управления рисками. Взаимосвязь сетей общего пользования с частными сетями, а также совместное использование информационных активов являются причинами возникновения затруднений при управлении доступом к информации и ее обработке. Кроме того, повсеместное использование мобильных устройств хранения данных (внешних накопителей), с записанными на них информационными активами, может снизить эффективность традиционных средств управления. Если организации применяют семейство стандартов СУИБ, то они могут продемонстрировать торговым партнерам фирмы и другим заинтересованным сторонам свою способность использовать единообразные и общеизвестные принципы информационной безопасности.

При проектировании и разработке информационных систем не всегда учитываются требования информационной безопасности. Часто предполагается обеспечить информационную безопасность впоследствии путем внедрения технического решения. Однако обеспечить информационную безопасность только с помощью технических средств невозможно, защита будет ограниченной и возможно неэффективной без поддержки соответствующего управления и процедур СУИБ. Интеграция системы безопасности с функционально законченной информационной системой может стать трудновыполнимой и дорогостоящей.

Внедрение СУИБ включает определение имеющихся средств управления, а также требует особой тщательности при проектировании и внимания к деталям. Например, средства управления доступом, которые могут быть техническими (логическими), физическими, административными (организационными) или комбинированными, обеспечивают гарантированную возможность разрешать и ограничивать доступ к информационным активам в соответствии с требованиями бизнеса и безопасности.

Успешное внедрение СУИБ имеет важное значение для защиты информационных активов организации и обеспечивает:

a) получение максимальной гарантии достаточной и непрерывной защиты информационных активов;

b) эксплуатацию структурированного и комплексного механизма определения и оценки рисков информационной безопасности, выбора и применения соответствующих средств управления, измерения и улучшения их эффективности;

c) непрерывное улучшение своей среды управления;

d) эффективное выполнение требований законодательных и нормативно-правовых актов.

4.5 Создание, мониторинг, эксплуатация и улучшение СУИБ

4.5.1 Краткий обзор

Организация для создания, мониторинга, эксплуатации и улучшения СУИБ должна выполнить следующие шаги:

a) идентифицировать информационные активы и соответствующие им требования безопасности (см. 4.5.2);

b) определить риски информационной безопасности (см. 4.5.3);

c) выбрать и внедрить соответствующие средства управления, необходимые для управления неприемлемым риском (см. 4.5.4);

d) проводить мониторинг, эксплуатировать и повышать эффективность средств управления безопасностью, связанных с информационными активами организации (см. 4.5.5).

Для обеспечения гарантий того, что СУИБ на постоянной основе эффективно защищает информационные активы организации, необходимо непрерывно повторять шаги (a) - (d), чтобы отслеживать изменения рисков, политик организации или бизнес-целей.

4.5.2 Определение требований информационной безопасности

В зависимости от общей политики, бизнес-целей, размера и территориального расположения организации требования информационной безопасности могут быть определены посредством интерпретации:

a) идентифицированных информационных активов и их важности;

b) потребности бизнеса в обработке, хранении и обмене информации;

c) требований законодательных и нормативно-правовых актов, а также договоров.

Систематически проводимое определение рисков для информационных активов организации включает анализ: угроз; уязвимостей и вероятности реализации угроз; потенциального влияния любого информационного инцидента безопасности на эти активы. Предполагается, что расходы на соответствующие средства управления безопасностью будут пропорциональны размеру предполагаемого ущерба бизнесу в случае материализации риска.

4.5.3 Определение рисков информационной безопасности

Для управления рисками информационный безопасности необходимы соответствующие методы определения и обработки рисков, которые могут включать расчет затрат и экономического эффекта, требования законодательных актов, интересы заинтересованных сторон и другие соответствующие входные данные и переменные.

Процесс определения рисков включает идентификацию, сравнительную оценку риска, и назначение им приоритетов в соответствии с критериями принятия риска и важностью целей для организации. Результаты определения рисков информационной безопасности помогут руководству принять решения относительно управления рисками

информационной безопасности, назначения приоритетов при управлении рисками информационной безопасности и внедрения соответствующих средств управления безопасностью для защиты от этих рисков.

Для определения значимости риска (для оценки риска) процесс определения рисков должен включать систематический метод оценки величины риска (анализ риска) и процесс сравнения предполагаемого риска с соответствующими критериями риска.

Определение риска должно выполняться периодически, это позволит своевременно учитывать изменения требований информационной безопасности и возникновение рискованных ситуаций, а также произошедшие существенные изменения, например, активов, угроз, уязвимостей, влияний, оценки риска. Для определения риска следует использовать методы, обеспечивающие сопоставимые и воспроизводимые результаты.

Для эффективного определения риска информационной безопасности должна быть четко определена область его действия. Определение риска информационной безопасности должно быть взаимосвязано с определениями рисков для других областей деятельности (при необходимости).

Рекомендации по управлению рисками информационной безопасности, в том числе рекомендации по определению, обработке и принятию рисков, обмену информацией относительно рисков, мониторингу рисков, а также краткий обзор рисков приведены в стандарте O‘z DSt ISO/IEC 27005.

4.5.4 Обработка рисков информационной безопасности

До начала обработки рисков организация должна установить критерии принятия рисков. Риск может быть принят, если, например, определено, что его уровень низкий или стоимость его обработки для организации экономически невыгодна. Эти критерии должны быть задокументированы.

После определения риска для каждого идентифицированного риска должно быть принято решение об его обработке. К возможным опциям обработки рисков относятся:

a) применение соответствующих средств управления для снижения рисков;

b) осознанное и объективное принятие рисков, если они однозначно удовлетворяют требованиям политики организации и критериям принятия рисков;

c) избежание рисков путем исключения действий, способствующих возникновению рисков;

d) разделение совместных рисков с другими сторонами, например, страховщиками или поставщиками.

После принятия решения об обработке рисков должны использоваться соответствующие средства управления, которые прежде были выбраны и внедрены.

4.5.5 Выбор и внедрение средств управления информационной безопасностью

После определения требований (4.5.2) и рисков (4.5.3) информационной безопасности для соответствующих информационных активов, а также после принятия решений по обработке рисков информационной безопасности (4.5.4) должны быть выбраны и внедрены соответствующие средства управления, обеспечивающие снижение этих рисков.

Средства управления следует проверить на предмет снижения ими рисков до приемлемого уровня, при этом принимая во внимание:

a) требования и ограничения национального и международного законодательства и норм;

b) цели организации;

c) действующие требования и условия;

d) стоимость внедрения и эксплуатации средств управления, задействованных в снижении рисков, пропорциональную требованиям и условиям организации;

e) для мониторинга, оценки, повышения производительности и эффективности средств управления информационной безопасностью, а также для поддержки целей организации должны быть внедрены соответствующие средства управления. Выбор и внедрение этих средств управления, а также их соответствие требованиям должны быть задокументированы в заявлении о применимости;

f) необходимость сбалансированности инвестиций во внедрение и эксплуатацию средств управления с вероятным ущербом, наносимым инцидентами информационной безопасности.

Средства управления, определенные в стандарте O‘z DSt ISO/IEC 27002, общепризнаны как лучшие, применимые и легко адаптируемые для использования в большинстве организаций разных размеров и различной сложности. Рекомендации по выбору и использованию средств управления, представленных в стандарте O‘z DSt ISO/IEC 27002, приведены в других стандартах семейства стандартов СУИБ.

Использование средств управления информационной безопасности следует предусматривать в технических заданиях на создание систем и в процессе проектирования. В противном случае могут потребоваться дополнительные издержки, решения могут быть менее эффективными и неблагоприятными, и возможно будет нельзя достичь необходимой безопасности. Средства управления могут быть выбраны из средств, рекомендованных в стандарте O‘z DSt ISO/IEC 27002, или из других соответствующих наборов средств управления, либо для удовлетворения соответствующих специфических потребностей организации могут быть разработаны новые средства управления. Необходимо иметь в виду, что некоторые средства управления не могут быть применимы во всех информационных системах или средах, а также во всех организациях.

В некоторых случаях для внедрения выбранной совокупности средств управления потребуется дополнительное время, поэтому в этот период времени уровень риска может стать более высоким, чем это было допустимо в предыдущий период. Во время внедрения средств управления риск не должен превышать пределы критериев допустимого риска. Заинтересованные стороны должны быть оповещены об уровне оцененного или потенциального риска в различных точках в период постепенного внедрения средств управления.

Следует иметь в виду, что достичь полной информационной безопасности, только установив средства управления, невозможно. Для поддержки целей организации следует дополнительно выполнять действия управления, в том числе мониторинг, оценку и улучшение эффективности и результативности средств управления информационной безопасностью.

Выбор и внедрение средств управления должны быть документально оформлены в заявлении о применимости, которое будет способствовать проверке соответствия этих средств требованиям.

4.5.6 Мониторинг, эксплуатация и повышение эффективности СУИБ

При эксплуатации и улучшении СУИБ организация должна вести мониторинг и оценивать деятельность, идущую вразрез с политикой и целями организации; полученные результаты должны отражаться в отчетах, предоставляемых руководству для анализа. Анализ СУИБ позволит удостовериться в том, что она содержит указанные средства управления, которые пригодны для обработки рисков в области действия СУИБ. Кроме того, на основе записей по результатам мониторинга этой области, будут предоставлены свидетельство о соответствии СУИБ требованиям и возможность оперативного контроля выполнения корректирующих и предупреждающих действий, а также действий по улучшению СУИБ.

4.5.7 Постоянное улучшение

Цель постоянного улучшения СУИБ заключается в том, чтобы увеличить вероятность достижения целей относительно сохранения конфиденциальности, доступности и целостности информации. Постоянное улучшение сфокусировано на поиске возможностей улучшения, при этом не делается допущения, что существующая деятельность управления - достаточно хороша или хороша настолько, насколько это возможно.

Действия по улучшению включают следущее:

a) анализ и оценку существующей ситуации с целью определения области улучшения;

b) определение целей улучшения;

c) поиск возможных решений для достижения целей;

d) оценку этих решений и выбор оптимального решения;

e) внедрение выбранного решения;

f) измерения, анализ и оценку результатов внедрения, проверку достижения целей;

g) документирование изменений.

Полученные результаты необходимо анализировать с целью определения дальнейших возможностей улучшения. Таким образом, процесс улучшения является непрерывной деятельностью, то есть эти действия повторяются часто. При определении возможностей улучшения могут использоваться отзывы потребителей и других заинтересованных сторон, аудиты и анализ СУИБ.

4.6 Критические факторы успеха СУИБ

Существует множество критических факторов, влияющих на успешное внедрение СУИБ, которая будет способствовать организации в достижении ее бизнес-целей. Примерами критических факторов успеха являются:

a) политика информационной безопасности, цели и деятельность, направленная на достижение целей;

b) методика и инфраструктура, необходимые для проектирования, внедрения, мониторинга, эксплуатации и улучшения информационной безопасности, соответствующие организационной культуре;

c) ощутимая поддержка и обязательства со стороны всех уровней управления, особенно высшего руководства;

d) понимание требований защиты информационных активов, достигаемое посредством управления рисками информационной безопасности (см. O‘z DSt ISO/IEC 27005);

e) степень осведомленности в области информационной безопасности, тренинги и обучающие программы, информирование всех служащих и других соответствующих сторон об их обязательствах в области информационной безопасности, изложенных в политиках информационной безопасности, стандартах и т.п., и их мотивация к соответствующим действиям;

f) эффективный процесс управления инцидентами информационной безопасности;

g) эффективный метод управления непрерывностью бизнеса;

h) система измерений, используемая для оценки выполнения управления информационной безопасностью и выдачи предложений по его улучшению.

СУИБ увеличивает вероятность того, что организация последовательно достигнет критических факторов успеха, необходимых для защиты ее информационных активов.

4.7 Преимущества семейства стандартов СУИБ

Основным преимуществом внедрения СУИБ является снижение рисков информационной безопасности (то есть уменьшение вероятности и/или влияния инцидентов информационной безопасности). В частности, преимущества для организации, реализованные в результате принятия семейства стандартов СУИБ и позволяющие достичь стабильного успеха, включают:

a) структурированную методику к поддержке процесса проектирования, внедрения, работы и эксплуатации комплексной и рентабельной, эффективной, интегрированной и встроенной СУИБ, которая удовлетворяет потребности организации посредством различных операций и подразделений;

b) помощь руководству в непрерывном контроле и надежном функционировании процесса управления информационной безопасностью в контексте управления корпоративными рисками и методов управления, включая обучение и тренинги владельцев бизнеса и систем в области комплексного подхода к управлению информационной безопасностью;

c) недирективный подход к использованию общепринятых международных стандартов в области информационной безопасности, позволяющий организациям самостоятельно выбирать и улучшать основные средства управления, которые соответствуют специфическим условиям их деятельности, и эксплуатировать эти средства независимо от внутренних и внешних изменений;

d) обеспечение универсальным языком и концептуальной основой информационной безопасности, облегчающими установление доверия с бизнес-партнерами, особенно когда они требуют предъявить сертификат соответствия СУИБ требованиям O‘z DSt ISO/IEC 27001 от аккредитованного органа по сертификации;

e) повышение доверия к организации заинтересованных сторон;

f) удовлетворение социальных потребностей и ожиданий;

g) большая эффективность управления экономическими инвестициями в информационную безопасность.

5 Семейство стандартов СУИБ

5.1 Общие положения

Семейство стандартов СУИБ состоит из взаимосвязанных стандартов, уже опубликованных или еще разрабатываемых, и содержит множество значимых структурных компонентов. Эти компоненты сосредоточены в стандартах, описывающих требования к СУИБ (O‘z DSt ISO/IEC 27001) и требования к органам по сертификации (O‘z DSt ISO/IEC 27006), выполняющих сертификацию СУИБ на соответствие требованиям O‘z DSt ISO/IEC 27001. В других стандартах

этого семейства содержатся руководящие указания по различным аспектам внедрения СУИБ, в том числе общие рекомендации по управлению, а также рекомендации для конкретных сфер деятельности. Взаимосвязи внутри семейства стандартов СУИБ показаны на рисунке 1.

Каждый стандарт из семейства стандартов СУИБ описывается ниже согласно своего типа (или роли) в этом семействе и номера ссылки. Стандарты этого семейства классифицированы и затем охарактеризованы как стандарты, содержащие:

a) обзор и терминологию (5.2);

b) требования (5.3);

c) общие руководящие указания (5.4);

d) руководящие указания для конкретных сфер деятельности (5.5).

5.2 Стандарты, содержащие обзор и терминологию

5.2.1 O‘z DSt ISO/IEC 27000 (настоящий стандарт)

Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Обзор и словарь

Область применения: В этом стандарте для организаций и физических лиц представлены:

a) обзор семейства стандартов СУИБ;

b) введение в СУИБ;

c) краткое описание процессов модели PDCA;

d) термины и определения, используемые во всех стандартах семейства СУИБ.

Цель: Описать основные принципы СУИБ, которые формируют предмет рассмотрения семейства стандартов СУИБ, и дать определения соответствующих терминов.

5.3 Стандарты, содержащие требования

5.3.1 O‘z DSt ISO/IEC 27001

Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования

Область применения: Этот стандарт устанавливает требования по разработке, внедрению, функционированию, мониторингу, анализу и совершенствованию документированной СУИБ в контексте общих бизнес-рисков организации. Стандарт определяет требования к внедрению средств управления безопасностью, адаптированных к индивидуальным потребностям организаций или их подразделений. Этот стандарт применим в организациях всех типов (например, в коммерческих предприятиях, некоммерческих организациях и государственных учреждениях).

Рисунок 1 – Взаимосвязи внутри семейства стандартов СУИБ

Цель: Установить нормативные требования по разработке и функционированию СУИБ, включая комплекс средств управления, осуществляющих управление рисками и их снижение для информационных активов, которые организация старается защитить с помощью СУИБ. Организации, имеющие СУИБ, могут провести их аудит и сертифицировать на соответствие требованиям O‘z DSt ISO/IEC 27001. Чтобы СУИБ соответствовала определенным требованиям, из приложения А стандарта O‘z DSt ISO/IEC 27001 должны быть выбраны, как часть процесса СУИБ и в соответствии с конкретными условиями, цели и средства управления. Цели и элементы управления, перечисленные в таблице А.1 O‘z DSt ISO/IEC 27001, заимствованы непосредственно из разделов 5 – 15 стандарта O‘z DSt ISO/IEC 27002.

5.3.2 O‘z DSt ISO/IEC 27006

Информационная технология. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью

Область применения: Этот стандарт устанавливает требования к органам аудита и сертификации СУИБ, дополняет требования стандарта O‘z DSt ISO/IEC 17021, и предоставляет руководство для указанных органов. Стандарт предназначен для оказания содействия органам, проводящим аудит и сертификацию СУИБ согласно O‘z DSt ISO/IEC 27001, в их аккредитации.

Цель: Дополнить требования стандарта O‘z DSt ISO/IEC 17021 требованиями по аккредитации органов сертификации, проводящих сертификацию СУИБ на соответствие требованиям стандарта O‘z DSt ISO/IEC 27001.

5.4 Стандарты, содержащие общие руководящие указания

5.4.1 O‘z DSt ISO/IEC 27002

Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью

Область применения: Этот стандарт содержит перечень общепринятых целей управления и современных средств управления, а также руководящие указания по выбору и внедрению средств управления, предназначенных для обеспечения информационной безопасности.

Цель: Предоставить руководящие указания по внедрению средств управления информационной безопасностью.

При этом в разделах 5 - 15 приведены конкретные рекомендации и руководящие указания по методам поддержки средств управления, определенных в разделах А.5 - А.15 O‘z DSt ISO/IEC 27001.

5.4.2 O‘z DSt ISO/IEC 27003

Информационная технология. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью

Область применения: Этот стандарт содержит полезные руководящие указания и предоставляет дополнительную информацию в области разработки, внедрения, функционирования, мониторинга, анализа, обслуживания и совершенствования СУИБ в соответствии с O‘z DSt ISO/IEC 27001.

Цель: Обеспечить применение процессного подхода для успешного внедрения СУИБ в соответствии с O‘z DSt ISO/IEC 27001.

5.4.3 O‘z DSt ISO/IEC 27004

Информационная технология. Методы обеспечения безопасности. Измерение эффективности системы управления информационной безопасностью

Область применения: Этот стандарт содержит руководство и рекомендации по разработке и использованию измерений для оценки эффективности СУИБ, управления целями и средствами управления, используемыми при внедрении и управлении информационной безопасностью в соответствии с O‘z DSt ISO/IEC 27001.

Цель: Предоставить методику измерения, позволяющую оценить эффективность СУИБ, которую необходимо измерять согласно O‘z DSt ISO/IEC 27001.

5.4.4 O‘z DSt ISO/IEC 27005

Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности

Область применения: Этот стандарт содержит руководящие указания по управлению рисками информационной безопасности. Методы, описанные в этом стандарте, поддерживают общие принципы, изложенные в O‘z DSt ISO/IEC 27001.

Цель: Предоставить руководство по внедрению подхода к управлению рисками, которое будет содействовать внедрению и выполнению надлежащим образом требований O‘z DSt ISO/IEC 27001 в области управления рисками информационной безопасности.

5.5 Стандарты, содержащие руководящие указания для конкретных сфер деятельности

5.5.1 O‘z DSt ISO/IEC 27011

Информационная технология. Методы обеспечения безопасности. Руководящие указания по управлению защитой информации организаций, предлагающих телекоммуникационные услуги

Область применения: Этот стандарт содержит руководящие указания, поддерживающие внедрение управления информационной безопасностью исключительно в организациях телекоммуникаций.

Цель: Адаптировать руководящие указания стандарта O‘z DSt ISO/IEC 27002 применительно только к организациям сферы телекоммуникаций, дополнив их требованиями в части управления в соответствии с приложением А стандарта O‘z DSt ISO/IEC 27001.

Приложение А
(справочное)

Глагольные формы для выражения положений

Каждый документ из семейства стандартов СУИБ сам по себе не налагает какие-либо обязательства на каждого его пользователя. Тем не менее, такие обязательства могут быть наложены, например, законодательством или договором. Для того, чтобы пользователь был способен выполнить требования документа, он должен вначале идентифицировать те требования, которые нужно обязательно выполнить. Пользователь также должен быть способен отличить эти требования от других рекомендаций, которые предоставляют ему определенную свободу выбора.

В таблице А.1 разъясняется, каким образом должны быть интерпретированы любые требования и рекомендации документов семейства стандартов СУИБ с точки зрения использованных в них глагольных форм для выражения положений.

Таблица А.1 – Использование глагольных форм для выражения положений в семействе стандартов СУИБ

Положение	Разъяснение
Требование	выражения «должен» и «не должен» означают, что требования должны быть выполнены строго в соответствии с документом и что какие-либо отклонения не допустимы
Рекомендация	выражения «следует» и «не следует» указывают на то, что среди нескольких возможностей рекомендуется использовать одну наиболее подходящую, не упоминая или исключая другие возможности, или что предпочтителен определенный образ действий, но не обязателен, или что (в отрицательной форме) определенная возможность или образ действий не одобряется, но и не запрещается
Разрешение	выражения «может» и «необязательно должен» указывают на образ действий, допустимый в рамках документа
Возможность	выражения «может» и «не может» означают возможность появления чего-то

Приложение B
(справочное)

Алфавитный указатель терминов на английском языке

Приложение С
(справочное)

Сведения о соответствии государственных стандартов Республики Узбекистан международным стандартам

Таблица С.1

Обозначение и наименование ссылочного государственного стандарта Республики Узбекистан	Степень соответствия	Обозначение и наименование соответствующего международного стандарта
O‘z DSt ISO/IEC 17021:2009 Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента	IDT	ISO/IEC 17021:2006 Оценка соответствия. Требования к органам, проводящим аудит и сертификацию систем менеджмента
O‘z DSt ISO/IEC 27001:2009 Информационные технологии. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования	IDT	ISO/IEC 27001:2005 Информационная технология. Методы обеспечения безопасности. Системы управления информационной безопасностью. Требования
O‘z DSt ISO/IEC 27002:2008 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью	IDT	ISO/IEC 27002:2005 Информационная технология. Методы обеспечения безопасности. Практические правила управления информационной безопасностью
O‘z DSt ISO/IEC 27003:2014 Информационная технология. Методы обеспечения безопасности. Руководство по внедрению системы управления информационной безопасностью	MOD	ISO/IEC 27003:2010 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	MOD	ISO/IEC 27004:2009 Информационная технология. Методы обеспечения безопасности. Управление информационной безопасностью. Измерения

Окончание таблицы С.1

Обозначение и наименование ссылочного государственного стандарта Республики Узбекистан	Степень соответствия	Обозначение и наименование соответствующего международного стандарта
O‘z DSt ISO/IEC 27005:2013 Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности	MOD	ISO/IEC 27005:2011 Информационная технология. Методы обеспечения безопасности. Управление рисками информационной безопасности
O‘z DSt ISO/IEC 27006:2013 Информационная технология. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью	MOD	ISO/IEC 27006:2007 Информационная технология. Методы обеспечения безопасности. Требования к органам аудита и сертификации систем управления информационной безопасностью
O‘z DSt ISO/IEC 27011:2014 Информационная технология. Методы обеспечения безопасности. Руководящие указания по управлению информационной безопасностью в организациях телекоммуникаций	MOD	ISO/IEC 27011:2008 Информационная технология. Методы обеспечения безопасности. Руководящие указания по управлению информационной безопасностью для организаций телекоммуникаций на основе ISO/IEC 27002
Примечание - В настоящей таблице использованы следующие условные обозначения степени соответствия стандартов: IDT - идентичная; MOD – модифицированная.		

УДК 681.324:006.354 ОКС 35.040 Т55

Ключевые слова: система управления информационной безопасностью, процессный подход, значимость, создание, мониторинг, эксплуатация, улучшение, критические факторы успеха, преимущества

Вр.и.о. директора
ГУП «UNICON.UZ» Х. Хасанов

Начальник научно-
исследовательского отдела
криптографии О. Ахмедова

Ведущий инженер
научно-исследовательского отдела
криптографии С. Абрамова

Младший научный сотрудник
научно-исследовательского отдела
криптографии Д. Джаматова

Нормоконтроль Л. Шаймарданова

СОГЛАСОВАНО

Начальник отдела
информационной безопасности
Государственного комитета связи,
информатизации и телекоммуникационных
технологий Республики Узбекистан

А. Гафуров
письмо от 29.04.2014 г.
№ 14-8/2564

СОГЛАСОВАНО

Первый заместитель начальника
Государственной инспекции по надзору
в сфере связи информатизации и
телекоммуникационных технологий

И. Ашуров
письмо от 10.04.2014 г.
№ 32-13/484