ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27034-2— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность приложений

Часть 2

Нормативная структура организации

(ISO/IEC 27034-2:2015, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

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

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 022 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 14 мая 2021 г. № 350-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27034-2:2015 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 2. Нормативная структура организации» (ISO/IEC 27034-2:2015 «Information technology — Security techniques — Application security — Part 2: Organization normative framework», IDT).

ИСО/МЭК 27034-2:2015 подготовлен подкомитетом 27 «Методы и средства обеспечения безопасности ИТ» Совместного технического комитета ИСО/МЭК СТК 1 «Информационные технологии».

При применении настоящего стандарта рекомендуется использовать вместо ссылочных международных стандартов соответствующие им национальные стандарты, сведения о которых приведены в дополнительном приложении ДА.

Дополнительные сноски в тексте стандарта, выделенные курсивом, приведены для пояснения текста оригинала

5 ВВЕДЕН ВПЕРВЫЕ

6 Некоторые положения международного документа, указанного в пункте 4, могут являться объектом патентных прав. Международная организация по стандартизации (ИСО) и Международная электротехническая комиссия (МЭК) не несут ответственности за идентификацию подобных патентных прав

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

Содержание

Введение

Общие положения

Организации должны обеспечивать защиту своей информации и технологических инфраструктур, чтобы сохранять свою конкурентоспособность. В настоящее время организации сталкиваются с постоянно растущей потребностью уделять внимание защите информации на уровне приложений. Системный подход к повышению уровня защиты приложений дает организациям основания полагать, что информация, используемая или хранимая приложениями, надежно защищена.

ИСО/МЭК 27034, состоящий из нескольких частей, определяет понятия, принципы, структуры, компоненты и процессы для оказания помощи организациям в планомерной интеграции мер обеспечения безопасности на протяжении жизненного цикла приложений.

Нормативная структура организации (НСО) является наиболее важным компонентом.

НСО — это внутренняя структура организации, включающая в себя совокупность передовых методов обеспечения безопасности приложений, используемых организацией. В нее входят основные компоненты, процессы, используемые этими компонентами, а также процессы менеджмента НСО. Она является основой обеспечения безопасности приложений организации, и все будущие решения по безопасности приложений должны приниматься с учетом этой структуры. НСО является основным источником данных для всех компонентов и процессов, связанных с обеспечением безопасности приложений организации.

В настоящем стандарте определены процессы, необходимые для системы менеджмента безопасности приложений организации. Описание этих процессов приведено в 5.4. В настоящем стандарте определены отвечающие за безопасность элементы приложений (процессы, роли и компоненты), которые должны быть интегрированы в НСО. Описание этих элементов приведено в 5.5.

В настоящем стандарте дано описание процесса аудита НСО, необходимого для проверки НСО и всех приложений на соответствие требованиям и средствам контроля НСО. Описание процесса аудита НСО приведено в 5.4.8.

Назначение

Целью настоящего стандарта является содействие организациям в создании, поддержке и проверке своих собственных НСО в соответствии с требованиями, установленными в настоящем стандарт[1)].

Настоящий стандарт предназначен для того, чтобы организации могли согласовывать или объединять свою НСО с корпоративной архитектурой организации и (или) системой менеджмента информационной безопасности. Однако внедрение системы менеджмента информационной безопасности, приведенной в ИСО/МЭК 27001, не является обязательным требованием для применения настоящего стандарта.

Целевая аудитория

Общие положения

Настоящий стандарт полезен для следующих групп лиц при осуществлении своих ролей в организации:

a) руководителей;

b) групп НСО;

c) экспертов в предметной области;

d) аудиторов.

Руководители

Руководители должны ознакомиться с настоящим стандартом, поскольку несут ответственность за:

a) повышение уровня безопасности приложений с помощью НСО и других подходов, приведенных в ИСО/МЭК 27034;

b) обеспечение соответствия НСО требованиям системы менеджмента информационной безопасности организации и требованиям безопасности приложений;

---

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

c) управление созданием НСО в организации;

d) обеспечение доступности НСО, а также передачу данных ответственным лицам и использование в проектах приложений надлежащих инструментальных средств и процедур в рамках всей организации;

e) определение соответствующих уровней управления, которым подчиняется группа НСО.

Группа НСО

Группа НСО несет ответственность за внедрение и обслуживание компонентов и процессов, связанных с безопасностью приложений, в рамках нормативной структуры организации. В обязанности группы НСО входят следующие мероприятия:

a) определение стоимости внедрения и обслуживания НСО;

b) определение компонентов и процессов, которые необходимо внедрить в НСО;

c) обеспечение соответствия внедренных компонентов и процессов приоритетам организации в отношении требований безопасности;

d) анализ аудиторских отчетов для определения соответствия НСО требованиям настоящего стандарта и требованиям организации;

e) предоставление процессов и инструментальных средств, удовлетворяющих требованиям стандартов, законов и нормативных актов в соответствии с регулятивным контекстом организации;

f) информирование всех лиц о проблемах безопасности, их обучение и осуществление надзора;

g) обеспечение соответствия проектов приложений организации требованиям НСО.

Команда разработчиков НСО

Специалисты, назначенные группой НСО для разработки и внедрения одного или нескольких элементов НСО, должны:

a) разрабатывать и внедрять запланированный элемент НСО;

b) определять, какое обучение необходимо действующим субъектам для использования элементов НСО;

c) помогать обеспечению адекватной подготовки действующих субъектов.

Эксперты в предметной области

Специалисты по обеспечению, приобретению и аудиту должны:

a) участвовать во внедрении и обслуживании НСО;

b) проверять эффективность и удобство использования НСО в ходе реализации проекта приложения;

c) предлагать новые компоненты и процессы.

Аудиторы

Аудиторы — это сотрудники, непосредственно занятые в процессах аудита, которые участвуют в процессах валидации и верификации НСО.

Примечание — Аудиторы могут быть внешними или внутренними по отношению к организации, в зависимости от задач и условий аудита, а также в соответствии с политикой аудита организации и требованиями соответствия.

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность приложений

Часть 2

Нормативная структура организации

Information technology. Security techniques.
Application security. Part 2. Organization normative framework

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт содержит подробное описание нормативной структуры организации (НСО) и рекомендации по ее внедрению в организации.

2 Нормативные ссылки

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

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

ISO/IEC 27005, Information technology — Security techniques — Information security risk management (Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности)

ISO/IEC 27034-1:2011, Information technology — Security techniques — Application security — Part 1: Overview and concepts (Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия)

Примечание — Дополнительная информация о связи ИСО/МЭК 27034 (все части) с другими стандартами приведена в ИСО/МЭК 27034-1:2011 (подраздел 0.5).

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 27034-1, ИСО/МЭК 27000 и ИСО/МЭК 27005.

Издание официальное

4 Сокращения

ЖЦБП — жизненный цикл безопасности приложений (ASLC);

ЭМЖЦБП — эталонная модель жизненного цикла безопасности приложений (ASLCRM);

НСП — нормативная структура приложений (ANF);

МОБП — меры обеспечения безопасности приложений (ASC);

ПМБП — процесс менеджмента безопасности приложений (ASMP);

НСО — нормативная структура организации (ONF).

5 Нормативная структура организации

5.1 Общие положения

Нормативная структура организации — это совокупность всех правил, политик, методов, ролей и инструментальных средств, используемых организацией. В каждой организации уже должна быть в некоторой степени задокументированная нормативная структура.

Концепция нормативной структуры организации, описанная в настоящем стандарте, представляет собой общеорганизационную структуру, содержащую подмножество процессов и компонентов организации, которые участвуют в обеспечении безопасности приложений и являются стандартными внутри организации.

Несмотря на то, что неформальная НСО является первым шагом на пути создания эффективной системы безопасности приложений организации, настоящий стандарт рекомендует создавать формализованную и стандартизированную НСО, как приведено в настоящем стандарте.

5.2 Назначение

Цели внедрения НСО состоят в следующем:

a) назначение лиц, ответственных за обеспечение безопасности приложений и установку процесса, который содействует повышению безопасности приложений;

b) создание условий для того, чтобы ответственные лица, принимающие решения, могли одобрять все элементы (компоненты, роли и процессы), связанные с безопасностью приложений, а участники и заинтересованные стороны могли принять эти условия;

c) минимизация сопротивления изменениям, вызванным внедрением новых элементов безопасности приложений;

d) стандартизация элементов безопасности приложений с целью обеспечения единообразия их внедрения и верификации во всей организации;

e) повышение уровня зрелости организации (в соответствии с ИСО/МЭК 15504 и другими стандартами, например SEI/CMMI[1)] с помощью формализации и доработки элементов безопасности приложений с целью их соответствия требованиям меняющейся среды организации;

f) создание механизмов, позволяющих более экономно внедрять соответствующие уровни безопасности, например с помощью повторного использования существующих утвержденных элементов безопасности приложений.

5.3 Принципы

Организации, создающие и поддерживающие компоненты и процессы НСО, должны руководствоваться следующими принципами:

a) содержимое НСО должно быть адаптировано к бизнес-потребностям организации;

b) любой элемент, входящий в НСО, должен быть одобрен группой НСО;

c) содержимое НСО должно быть доступно и распространяться по всей организации;

d) поскольку контекст угроз меняется непрерывно и без предупреждения, организации должны быть готовы обновлять НСО в ответ на эти изменения;

e) НСО должна быть проверяемой.

[1)] *Модель зрелости для программной и системной инженерии (SEI/CMMI).*

5.4 Процесс менеджмента нормативной структуры организации

5.4.1 Общие положения

Организация должна определять, внедрять, поддерживать и улучшать процесс менеджмента НСО на уровне всей организации.

Процесс менеджмента НСО состоит из шести подпроцессов.

Четыре из них являются адаптированной версией процессов «Планирование—Осуществление—Проверка—Действие» из общей методологии PDCA[1)] (Plan—Do—Check—Act) и предназначены для разработки и внедрения элементов безопасности приложений в НСО.

В таблице 1 приведено соответствие подпроцессов менеджмента НСО четырем этапам методологии PDCA и подпроцессам системы менеджмента информационной безопасности.

Таблица 1 — Сопоставление этапов PDCA, подпроцессов менеджмента информационной безопасности и подпроцессов менеджмента НСО, участвующих в обеспечении безопасности приложений

Этап PDCA	ИСО/МЭК 27001 Процесс менеджмента информационной безопасности	ИСО/МЭК 27034 Процесс менеджмента НСО
Планирование	Планирование	Проектирование НСО
Осуществление	Поддержка/эксплуатация	Внедрение НСО
Проверка	Оценка эффективности	Мониторинг и оценка НСО
Действие	Улучшение	Улучшение НСО

Кроме того, подпроцесс «Создание группы НСО» используется в первую очередь для того, чтобы организовать группу НСО и продемонстрировать ответственный подход соответствующих руководителей к обеспечению безопасности приложений. Наконец, подпроцесс «Аудит НСО» используется для проверки НСО и приложений на соответствие требованиям и средствам управления НСО.

Организация должна итеративно выполнять процесс менеджмента НСО, чтобы постепенно внедрить НСО. Отдавая приоритет более важным элементам в каждой новой итерации, можно снизить негативные последствия и быстрее получить положительный результат.

Графическое представление процесса менеджмента НСО приведено на рисунке 1. На рисунке показано, как этот процесс связан с другими процессами менеджмента организации и процессом менеджмента безопасности приложений, который использует НСО для внедрения мер обеспечения безопасности приложений в проекты приложений.

[1)] *Планирование — осуществление — проверка — действие (PDCA).*

Рисунок 1 — Процесс менеджмента НСО

5.4.2 Использование диаграмм RACI для описания мероприятий, ролей и обязанностей

В настоящем стандарте для назначения ролей и обязанностей по выполнению мероприятий, входящих в процессы, используются диаграммы RACI[1)] (Responsible —Accountable — Consulted — Informed). С помощью таких диаграмм определяются действующие субъекты, ответственные, отчитывающиеся, консультирующие и сообщающие о выполнении действий. Для описания обязанностей действующих субъектов используются сокращения, приведенные в таблице 2.

Таблица 2 — Сокращения, используемые в диаграммах RACI для описания обязанностей действующих субъектов

Код	Обязанность
R	Ответственный за выполнение действия
A	Отчитывающийся за выполнение действия
C	Консультирующий во время выполнения действия
I	Сообщающий о выполнении действия

[1)] *Ответственный за выполнение действия — Отчитывающийся за выполнение действия — Консультирующий во время выполнения действия — Сообщающий о выполнении действия.*

Использование диаграмм RACI в организациях, вводящих настоящий стандарт, не является обязательным. Организации должны использовать рекомендации, установленные в настоящем стандарте, с учетом собственных методов определения ролей и обязанностей.

Очень важно, чтобы организация определила ответственных, отчитывающихся, консультирующих и сообщающих о выполнении действия. Приведенные ниже таблицы 3—17 могут быть использованы при разработке и внедрении НСО.

5.4.3 Создание группы нормативной структуры организации

5.4.3.1 Назначение

Назначение данного процесса заключается в создании группы НСО, предоставлении группе полномочий и ресурсов, необходимых для разработки, внедрения и улучшения НСО, а также для демонстрации ответственного подхода соответствующих руководителей к обеспечению безопасности приложений.

5.4.3.2 Результаты

Результатами успешного выполнения данного процесса являются:

a) определение ролей и обязанностей членов группы НСО;

b) назначение кандидатов на каждую роль;

c) предоставление группе НСО официальных полномочий на создание и поддержку НСО и распространение этой информации внутри организации;

d) назначение группы НСО, ответственной за внедрение, поддержку качества и использование НСО в организации;

e) предоставление группе НСО необходимых ресурсов для выполнения своих обязанностей;

f) предоставление группе НСО достаточных полномочий для поддержки необходимой внутренней коммуникации.

5.4.3.3 Мероприятия по внедрению

Таблица 3 — Диаграмма RACI для внедрения процесса «Создание группы НСО»

Мероприятия по внедрению	Руководители
1) Определение ролей и обязанностей членов группы НСО	A/R
2) Назначение кандидатов на каждую роль	A/R
3) Предоставление группе НСО официальных полномочий на создание и поддержку НСО и распространение этой информации внутри организации	A/R
4) Назначение группы НСО, ответственной за внедрение, поддержку качества и использование НСО в организации	A/R
5) Предоставление группе НСО необходимых ресурсов для выполнения своих обязанностей	A/R
6) Предоставление группе НСО достаточных полномочий для поддержки необходимой внутренней коммуникации	A/R

5.4.3.4 Мероприятия по верификации

Таблица 4 — Диаграмма RACI для верификации процесса «Создание группы НСО»

Мероприятия по верификации	Руководители	Аудиторы
1) Проверка поступления официальных сообщений от ответственных руководителей, подтверждающих то, что были достигнуты результаты подпроцессов a), b), c) и d)	A	R
2) Оценка по официальным сообщениям ответственных руководителей достижения результатов подпроцессов e) и f)	A	R

5.4.4 Проектирование нормативной структуры организации

5.4.4.1 Назначение

Назначение данного процесса заключается в том, чтобы определить цели системы безопасности приложений, выбрать, какие элементы должны быть реализованы в НСО в рамках текущей итерации процесса менеджмента НСО, и создать проект этих элементов.

5.4.4.2 Результаты

Результатами успешного выполнения данного процесса являются:

a) определение объема текущей итерации процесса менеджмента НСО, а также последующее утверждение их ответственными руководителями и передача информации ответственным лицам;

b) разработка элементов НСО, входящих в данную итерацию.

5.4.4.3 Мероприятия по внедрению

Таблица 5 — Диаграмма RACI для внедрения процесса «Проектирование НСО»

Мероприятия по внедрению	Руководители	Группа НСО
1) Определение цели системы безопасности приложений	A	R
2) Определение объема и стратегии реализации текущей итерации процесса менеджмента НСО	A	R
3) Определение направления развития системы безопасности приложения организации, назначение приоритетов и составление плана		A/R
4) Определение инструментальных средств и уровня конфиденциальности информации, используемой приложениями, а также интегрирование их в информационную архитектуру организации		A/R
5) Разработка элементов НСО		A/R

5.4.4.4 Мероприятия по верификации

Таблица 6 — Диаграмма RACI для верификации процесса «Проектирование НСО»

Мероприятия по верификации	Руководители	Аудиторы
1) Подтверждение того, что объем текущей итерации процесса менеджмента НСО определен и утвержден ответственными руководителями, а информация передана ответственным лицам	A	R
2) Подтверждение того, что элементы НСО, входящие в данную итерацию, спроектированы правильно	A	R

5.4.4.5 Рекомендации

Исходными данными для данного процесса являются:

a) результаты процесса менеджмента рисков безопасности организации, например, цели или планы по развитию безопасности на уровне организации;

b) результаты процесса «Улучшение НСО», например, документально подтвержденная потребность в доработке элементов НСО или разработке новых элементов НСО;

c) результаты процесса «Аудит НСО»;

d) результаты аудита информационной безопасности организации;

e) потребности в обучении, стратегия, показатели, политики, новая информация об атаках и минимизации их последствий;

f) другие стандарты ИСО/МЭК, в том числе стандарты, относящиеся к поставкам (ИСО/МЭК 27036), оценке (ИСО/МЭК 15408), гарантиям (ИСО/МЭК 15026), процессам жизненного цикла программных средств (ИСО/МЭК 12207), процессам жизненного цикла системы (ИСО/МЭК 15288); см. ИСО/МЭК 27034-1:2011 (подраздел 0.5 и рисунок 1).

Описание элементов НСО, которые необходимо разработать, приведено в 5.5. Конкретные рекомендации по разработке этих элементов также содержатся в 5.5.

Элементы НСО должны быть разработаны и внедрены в ходе итеративного процесса. В ходе этого процесса группе НСО следует:

a) определить приоритетные элементы исходя из приоритетов организации и имеющихся ресурсов;

b) назначить ответственных лиц и выделить необходимые ресурсы для разработки элементов, входящих в данную итерацию;

c) контролировать и проверять проекты элементов НСО;

d) интегрировать процессы НСО в бизнес-процессы организации;

e) обеспечить соответствие политики безопасности приложений НСО другим политикам организации и требованиям системы менеджмента информационной безопасности организации;

f) обеспечить соответствие НСО архитектуре безопасности организации, информационной архитектуре и бизнес-архитектуре;

g) обеспечить соответствие показателей эффективности менеджмента рисков НСО другим показателям эффективности, используемым в организации;

h) обеспечить соответствие целей менеджмента рисков НСО целям и стратегиям организации;

i) обеспечить соблюдение правовых и нормативных требований;

j) обеспечить информирование всех заинтересованных сторон о результатах своей деятельности;

k) создать репозиторий данных, которое являлось бы авторитетным источником для консолидации и передачи информации об НСО и всех его элементах;

l) определить механизмы коммуникации и создания отчетности (внутренние, внешние, интерфейсы с проектами приложений и т. д.);

m) информировать руководство о возможностях организации в достижении соответствия требованиям настоящего стандарта, определив политику менеджмента безопасности приложений.

Примечание — Не следует ожидать, что каждый работник или партнер организации будет знаком с настоящим стандартом. Однако, следует требовать от указанных лиц выполнения условий, соответствующих политике.

При утверждении объема итерации процесса менеджмента НСО ответственные руководители должны:

a) удостовериться, что НСО и процессы менеджмента, входящие в нее, совместимы со стратегическим направлением, задачами в области информационной безопасности и политикой организации;

b) убедиться, что НСО соответствует корпоративной архитектуре организации и поддерживает ее.

При проверке правильности разработки элементов НСО в рамках текущей итерации, аудиторы могут опираться на следующие критерии:

a) определенный объем и стратегию реализации текущей итерации процесса менеджмента НСО;

b) определенные стратегические позиции в сфере безопасности приложений организации, приоритеты и планы;

c) установленные политики менеджмента безопасности приложений;

d) набор инструментальных средств и уровень конфиденциальности (с точки зрения конфиденциальности, целостности и доступности) информации, используемой приложениями, интегрированными в информационную архитектуру организации;

e) определенные роли для проекта внедрения в НСО каждого компонента и процесса;

f) назначенные на эти роли действующие субъекты;

g) результаты мониторинга проектов;

h) механизмы коммуникации и отчетности.

5.4.5 Внедрение НСО

5.4.5.1 Назначение

Назначение данного процесса заключается во внедрении элементов НСО, разработанных в рамках текущей итерации процесса менеджмента НСО, предоставлении решений по обеспечению безопасности приложений, таких как компоненты и процессы, и распространении их по всей организации в качестве обязательных процедур, услуг и руководящих принципов по обеспечению безопасности приложений.

5.4.5.2 Результаты

Успешным результатом данного процесса являются разработка и внедрение элементов НСО, а также обучение соответствующих действующих субъектов использованию этих элементов НСО.

5.4.5.3 Мероприятия по внедрению

Таблица 7 — Диаграмма RACI для внедрения процесса «Внедрение НСО»

Мероприятия по внедрению	Группа НСО	Команда разработчиков элемента НСО	Эксперты в предметной области
a) Анализ влияния и сложности разработки и внедрения элементов НСО, разработанных в рамках текущей итерации процесса менеджмента НСО	A/R		C
b) Для каждого разработанного элемента НСО:			
1) назначение команды разработчиков	A/R		
2) объяснение цели руководителей и указание направления команде разработчиков	A/R		
3) выделение достаточного количества ресурсов для команды разработчиков	A/R	C	
4) разработка и внедрение элемента НСО	A	R	C
5) определение того, какое обучение необходимо действующим субъектам для использования элемента НСО		A/R	C
6) обеспечение адекватной подготовки действующих субъектов	A/R	C	C

5.4.5.4 Мероприятия по верификации

Таблица 8 — Диаграмма RACI для верификации процесса «Внедрение НСО»

Мероприятия по верификации	Группа НСО	Аудиторы	Эксперты в предметной области
1) Подтверждение того, что элементы НСО разработаны и внедрены в соответствии с ожидаемыми результатами процесса «Проектирование НСО»	A	R	C
2) Подтверждение того, что соответствующие действующие субъекты прошли обучение, определенное командой разработчиков элемента НСО	A	R	C

5.4.5.5 Рекомендации

Для осуществления данного процесса должны использоваться следующие исходные данные:

a) стратегия внедрения текущей итерации процесса менеджмента НСО;

b) проект элементов НСО для текущей итерации.

В случае если организация предпочитает передавать разработку на аутсорсинг или приобретать какие-либо элементы НСО, влияющие на соответствие требованиям НСО, следует убедиться, что требования к управлению процессом, установленные группой НСО, были переданы ответственным лицам и выполняются организациями, которым была передана на аутсорсинг разработка элементов или у которых они приобретаются.

При назначении группы разработчиков для внедрения элемента НСО группа НСО должна предоставить разработчикам необходимые ресурсы для разработки конкретного элемента и привлечь квалифицированных сотрудников, главным образом экспертов в предметной области.

Пример — Экспертами в предметной области могут являться эксперты в области юриспруденции, судебные эксперты, технические специалисты, эксперты по криптографии, специалисты по режиму конфиденциальности.

При проверке того, что спроектированные элементы НСО разработаны и внедрены, аудиторы могут применять следующие критерии:

a) управление проектами НСО и инвестициями в безопасность приложений;

b) создание механизмов коммуникации и отчетности НСО;

c) использование интерфейсов в проектах безопасности приложений для доступа к элементам НСО;

d) информирование о важности эффективного менеджмента безопасности приложений в соответствии с системой менеджмента информационной безопасностью организации;

e) документирование и передача информации в соответствии с ИСО/МЭК 27001:2013;

f) внедрение элементов НСО для всех критически важных приложений, в зависимости от стратегии внедрения НСО;

g) подотчетность всех, кто связан с внедрением и использованием НСО.

Кроме того, для каждого разработанного элемента НСО аудиторы могут учитывать следующие критерии:

a) идентификацию владельца;

b) цели и область управления;

c) компетентность лиц, выполняющих работу;

d) обучение действующих субъектов для использования элемента НСО;

e) внедрение элемента НСО и управление им.

Конкретные рекомендации по внедрению некоторых элементов НСО содержатся в 5.5.

5.4.6 Мониторинг и оценка нормативной структуры организации

5.4.6.1 Назначение

Назначение данного процесса заключается в проверке компонентов и процессов НСО с целью подтверждения того, что они продолжают правильно выполнять свою задачу и используются в соответствии с политикой безопасности приложений организации.

5.4.6.2 Результаты

Результатами успешного выполнения данного процесса являются:

a) документально подтвержденная информация, которую можно использовать в качестве доказательства наличия результата проверок;

b) выявление и регистрация элементов НСО, которые необходимо улучшить.

5.4.6.3 Мероприятия по внедрению

Таблица 9 — Диаграмма RACI для внедрения процесса «Мониторинг и оценка НСО»

Мероприятия по внедрению	Группа НСО	Эксперты в предметной области
1) Определение стандартных методов измерения, анализа и оценки элементов НСО для обеспечения достоверности и повторяемости результатов	A/R	C
2) Отслеживание изменения (см. Рекомендации)	A/R	
3) Оценка элементов НСО с использованием определенных стандартных методов измерения, анализа и оценки, чтобы понять, работают ли они должным образом	A/R	C
4) Хранение документально подтвержденной информации в качестве доказательства наличия результата проверок	A/R	
5) Определение и регистрирование элементов НСО, которые требуется улучшить	A/R	C
6) Отчетность, по мере необходимости, о требуемых улучшениях элементов НСО перед командами, отвечающими за проект приложения	A/R	

5.4.6.4 Мероприятия по верификации

Таблица 10 — Диаграмма RACI для верификации процесса «Мониторинг и оценка НСО»

Мероприятия по верификации	Группа НСО	Аудиторы
1) Проверка наличия и качества документально подтвержденной информации, используемой в качестве доказательства наличия результатов проверок	A	R
2) Проверка наличия и качества документально подтвержденной информации о необходимых улучшениях элементов НСО	A	R

5.4.6.5 Рекомендации

Мониторинг и оценка НСО должны осуществляться через запланированные промежутки времени или после конкретных изменений в рамках всей организации, чтобы система оставалась пригодной, адекватной и эффективной.

Для осуществления этого процесса необходимо использовать следующие исходные данные:

a) результаты процесса оценки рисков информационной безопасности организации;

b) изменения специфики НСО организации;

c) результаты аудита НСО;

d) замечания заинтересованных сторон;

e) состояние предупреждающих и корректирующих действий;

f) результаты измерений эффективности;

g) данные об инцидентах безопасности приложения.

В качестве одного из важнейших источников информации для постоянного улучшения качества и эффективности МОБП, используемых в проектах, должна быть использована обратная связь от проектов приложений.

Примеры

1 Значение атрибута «стоимость» МОБП, как правило, является приблизительной оценкой и может быть определено более точно с помощью обратной связи от проектов приложений.

2 В связи с тем, что в организации постоянно происходят изменения в технологическом контексте, некоторые МОБП со временем перестают отвечать требованиям безопасности новых проектов приложений. В конечном итоге они устаревают и удаляются из библиотеки МОБП организации. Это позволяет предотвратить ситуацию, когда устаревшая МОБП превращается в уязвимость.

Отслеживаемые элементы НСО содержат артефакты проектов приложений. Осуществляя мониторинг этих элементов, группа НСО обеспечивает корректную работу проектов приложений согласно ПМБП, в частности гарантирует, что они:

a) правильно используют компоненты НСО;

b) обеспечивают целевые уровни доверия приложений и фактические уровни доверия приложений;

c) проводят периодическую оценку риска приложения.

Группа НСО должна выделять достаточное количество ресурсов и сотрудников для мониторинга и оценки элементов НСО, особенно экспертов в предметной области, подходящих для конкретного элемента НСО.

Пример — Экспертами в предметной области могут являться эксперты в области юриспруденции, судебные эксперты, технические специалисты, эксперты по криптографии, специалисты по режиму конфиденциальности.

Во время проверки правильности осуществления процесса мониторинга и оценки НСО, аудиторы могут применять следующие критерии:

a) методы определения и проверки мониторинга, измерения, анализа и оценки для обеспечения достоверности результатов;

b) учет решений, касающихся постоянного улучшения и возможных изменений НСО;

c) документально подтвержденную информацию, доказывающую наличие результатов проверок;

d) измерение и мониторинг элементов НСО;

e) оценку эффективности действий.

5.4.7 Улучшение нормативной структуры организации

5.4.7.1 Назначение

Назначение данного процесса заключается в следующем:

a) повышение удобства использования, целесообразности, адекватности и эффективности НСО;

b) добавление недостающих элементов, которые необходимо внедрить в связи с изменениями в организации;

c) обеспечение соответствия НСО системе менеджмента информационной безопасности организации.

5.4.7.2 Результаты

Результатами успешного выполнения данного процесса являются:

a) улучшение элементов НСО;

b) обнаружение необходимости доработки элементов НСО или разработки новых элементов НСО;

c) корректное документирование изменений в элементах НСО и передача документации ответственным лицам.

5.4.7.3 Мероприятия по внедрению

Таблица 11 — Диаграмма RACI для внедрения процесса «Улучшение НСО»

Мероприятия по внедрению	Группа НСО	Команда разработчиков элемента НСО	Эксперты в предметной области
1) Внесение ранее определенных необходимых улучшений элементов НСО	A	R	C
2) Оценка необходимости доработки элементов НСО или разработки новых элементов НСО	A	R	C
3) Документирование таких потребностей и передача информации о них процессу «Проектирование НСО»	A	R	C
4) Внесение изменений с помощью организационных процессов, таких как управление изменениями, управление конфигурацией и т. д.	A/R		
5) Подтверждение того, что информация об улучшениях, такая как цель, задачи, требования безопасности, на которые они направлены, описание и критерии верификации, должным образом задокументирована и передана ответственным лицам	A/R		

5.4.7.4 Мероприятия по верификации

Таблица 12 — Диаграмма RACI для верификации процесса «Улучшение НСО»

Мероприятия по верификации	Группа НСО	Аудиторы
1) Подтверждение того, что ранее определенные необходимые улучшения элементов НСО были внесены	A	R
2) Подтверждение того, что любая необходимость в доработке элементов НСО или разработке новых элементов НСО задокументирована	A	R
3) Подтверждение того, что изменения, внесенные в элементы НСО, задокументированы должным образом и переданы ответственным лицам	A	R
4) Проверка того, правильно ли были внесены изменения, с помощью организационных процессов, таких как управление изменениями, управление конфигурацией и т. д.	A	R

5.4.7.5 Рекомендации

Организация должна использовать для эффективного внесения изменений процессы менеджмента информационной безопасности, такие как управление, планирование и оценка эффективности.

В качестве исходных данных для этого процесса можно использовать результаты процесса «Мониторинг и оценка НСО», например:

a) документально подтвержденную информацию, которую можно использовать в качестве доказательства наличия результата проверок;

b) документально подтвержденную информацию о необходимости улучшения элементов НСО.

Группа НСО должна выделить достаточное количество ресурсов и сотрудников для улучшения элементов НСО, особенно экспертов в предметной области, подходящих для конкретного элемента НСО.

Пример — Экспертами в предметной области могут являться эксперты в области юриспруденции, судебные эксперты, технические специалисты, эксперты по криптографии, специалисты по режиму конфиденциальности.

Во время проверки правильности осуществления процесса улучшения НСО аудиторы могут применять следующие критерии:

a) оценку необходимости планирования действий для устранения рисков и реализации возможностей;

b) внедрение и использование этих действий в НСО, если это возможно;

c) реализацию возможностей для улучшения;

d) управление изменениями;

e) информацию об улучшениях, такую как цель, задачи, требования безопасности, на которые они направлены, описание и критерии верификации.

5.4.8 Аудит нормативной структура организации

5.4.8.1 Назначение

Назначение данного процесса заключается в определении степени соответствия НСО требованиям безопасности приложений организации, в частности политике менеджмента безопасности приложений организации. Это особенно важно для организаций, которым необходимо обеспечить соответствие их НСО требованиям другой НСО, например НСО головной или регулирующей компании.

Пример — Правительство может определить НСО с минимальными требованиями для всех государственных учреждений. В этом случае НСО государственного учреждения должна соответствовать НСО правительства, т. е. его система должна будет выполнять как минимум требования НСО правительства. Соответствие можно проверить в ходе аудита НСО учреждения.

5.4.8.2 Результаты

Результатами успешного выполнения данного процесса являются:

a) внедренная и действующая программа аудита НСО;

b) проверка элементов НСО в соответствии с программой;

c) должным образом задокументированные и переданные ответственным лицам результаты аудита;

d) использование результатов аудита для постоянного улучшения НСО.

5.4.8.3 Мероприятия по внедрению

Таблица 13 — Диаграмма RACI для внедрения процесса «Аудит НСО»

Мероприятия по внедрению	Руководители	Аудиторы	Группа НСО	Эксперты в предметной области
1) Внедрение и управление программой аудита НСО для интеграции аудиторской деятельности НСО в существующие процессы аудита	A	R	C	C
2) Обеспечение должного уровня подготовки аудиторов для проведения аудита НСО	A/R			C
3) Проведение аудита НСО	A	R	C	C
4) Выявление основных причин несоответствия и поиск решений по результатам аудита	I	A	C	R
5) Документирование результатов аудита и передача их ответственным лицам	A	R	I	
6) Подтверждение того, что результаты аудита используются в качестве исходных данных для процесса «Мониторинг и оценка НСО»		A/R	C	

5.4.8.4 Мероприятия по верификации

Таблица 14 — Диаграмма RACI для верификации процесса «Аудит НСО»

Мероприятия по верификации	Руководители	Внешний аудитор
1) Обеспечение корректного выполнения аудита НСО в соответствии с аудиторской программой НСО	A	R

5.4.8.5 Рекомендации

Ответственные руководители, помимо рекомендаций, приведенных в ИСО/МЭК 27007, должны выполнять программу аудита НСО и управлять ею, проводить аудит и обеспечивать компетентность аудиторов.

Во время внедрения программы аудита НСО руководство должно проанализировать уже существующие в организации процессы аудита, в частности процесс аудита системы менеджмента информационной безопасности, если таковой имеется, и разработать стратегию согласования или интеграции процесса аудита НСО с существующими процессами. Руководству также необходимо рассмотреть возможность использования руководящих принципов по аудиту систем управления, приведенных в ИСО 19011:2011 (подраздел 5.1).

Группа НСО должна определить конкретные элементы НСО для проверки и то, какими конкретными мероприятиями необходимо дополнить существующий процесс аудита для достижения поставленных руководством задач по программе аудита.

Программа аудита НСО нуждается не только в одобрении ответственных руководителей, но и в ресурсах и независимости, чтобы объективно оценивать соответствие НСО требованиям безопасности приложений организации, таким как:

a) четко определенные по диаграмме RACI (или аналогичными методами) обязанности и их доведение до сведения ответственных лиц;
b) экономическая эффективность и обновление элементов НСО;
c) соблюдение процесса управления изменениями;
d) завершенность подпроцессов менеджмента НСО;
e) выполнение верификации каждого подпроцесса менеджмента НСО;
f) учет результатов предыдущих аудитов и оценок рисков.

Для осуществления данного процесса должны использоваться следующие исходные данные:

a) результаты предыдущих аудитов и оценок рисков;
b) запросы, предоставляемые системой менеджмента информационной безопасности.

Группа НСО должна выделять необходимые ресурсы для проведения аудита элементов НСО, особенно экспертов в предметной области, подходящих для проведения аудита элементов НСО.

Пример — Экспертами в предметной области могут являться эксперты в области юриспруденции, судебные эксперты, технические специалисты, эксперты по криптографии, специалисты по режиму конфиденциальности.

Внешние аудиторы, уполномоченные подотчетными руководителями, должны подтвердить, что процесс аудита НСО был выполнен с учетом:

a) созданной программы аудита;
b) утвержденной программы аудита и выделенных ресурсов;
c) отчетов о результатах предыдущего аудита НСО;
d) списка основных причин несоответствий и решений;
e) свидетельства решений для мониторинга;
f) улучшений процесса аудита.

Примечание — Аудиторы могут быть внешними или внутренними, но они не должны являться работниками службы безопасности приложений организации или входить в группу НСО. Как и в случае с любым другим процессом, необходимо обеспечить разделение служебных обязанностей, чтобы были отдельные ответственные за внедрение и верификацию данного процесса.

5.5 Элементы нормативной структуры организации

5.5.1 Общие положения

В НСО входят различные элементы, такие как компоненты и процессы для удовлетворения потребностей организации в безопасности приложений. Нормативная структура организации (упрощенная) приведена на рисунке 2.

Рисунок 2 — Нормативная структура организации (упрощенная)

Примечание — В рамках настоящего стандарта рассматриваются два типа элементов: компоненты и процессы. Компоненты представлены на рисунке 2 в виде прямоугольников, а процессы изображены в виде прямоугольников с закругленными углами.

5.5.2 Компонент бизнес-контекста

5.5.2.1 Назначение

Данный компонент помогает идентифицировать риски безопасности и определяет требования, вытекающие из коммерческой деятельности организации, а также предоставляет значения, используемые в атрибуте МОБП «Направленный на требования». Он позволяет внедрить утвержденный стандартизированный метод снижения рисков, связанных с коммерческой деятельностью организации.

5.5.2.2 Описание

Бизнес-контекст — это список и задокументированное описание всех бизнес-процессов, стандартов и лучших методов работы, используемых в организации, которые могут оказать влияние на проекты приложений. Подобная деятельность подвержена риску, поэтому организация должна определить требования безопасности для снижения рисков. МОБП должны создаваться с учетом этих требований. Разработчики МОБП должны обосновать, для чего предназначена мера обеспечения безопасности

приложений, т. е. для выполнения какого требования безопасности внедряется МОБП. Необходимую информацию можно найти в компоненте бизнес-контекста НСО.

Примеры

1 Политика безопасности организации, как правило, является прямым источником требований безопасности. Некоторые из них имеют отношение к безопасности приложений. Несоответствие политике безопасности влечет за собой риск, неприемлемый для владельца приложения. МОБП могут разрабатываться для удовлетворения конкретных требований политики безопасности.

2 Бизнес-процесс для создания самолетов в области аэронавтики несет высокий уровень риска и, следовательно, содержит множество требований безопасности. В результате, как правило, в приложения, связанные с этим процессом, будет внедряться множество МОБП.

5.5.2.3 Содержание

Бизнес-контекст должен предоставить:

a) список всех сфер деятельности организации, осуществляемой во всех подразделениях организации, где будут внедряться или использоваться приложения;

b) список процессов, политик и лучших методов работы для всех сфер деятельности организации, в которых будут использоваться приложения, например:

1) процессы управления бизнесом, проектами, развитием, анализом рисков, бизнес-операциями, аудитом, контролем и изменениями;

2) политика безопасности организации;

3) перечень информационных активов организации с их уровнем конфиденциальности;

4) методы разработки, используемые в организации;

5) лучшие методы работы для всех языков программирования, используемых организацией и перечисленных в технологическом контексте;

6) стандарты, например стандарты ИСО/МЭК и производственные стандарты, которым организация обязалась соответствовать;

c) список рисков, сопутствующих вышеупомянутым процессам, политикам и лучшим методам работы и имеющих отношение к безопасности приложений;

d) список требований безопасности для снижения вышеуказанных рисков;

e) рекомендации и руководящие принципы по разработке МОБП, в том числе:

1) список атрибутов МОБП, которые должны или могут использоваться для описания МОБП;

2) сопоставление с атрибутами, описанными в ИСО/МЭК 27034-5;

3) в зависимости от обстоятельств, набор допустимых значений, правил, номенклатуры и зависимостей для каждого атрибута.

5.5.2.4 Рекомендации

Информация для создания данного компонента НСО должна быть получена путем анализа рисков информационной безопасности. Организациям, которые провели анализ рисков информационной безопасности в соответствии с руководящими принципами ИСО/МЭК 27001:2013 и процессом менеджмента рисков, предлагаемым в ИСО/МЭК 27005:2011, потребуются минимальные усилия для создания данного компонента.

Список информационных активов организации с их уровнем конфиденциальности необходимо составлять исходя из информационной архитектуры организации. В ИСО/МЭК 27001:2013 (пункт А.8.1.1) этот процесс называется «инвентаризацией активов».

Для эффективного менеджмента рисков список информационных активов организации должен быть достаточно детализированным. Вся информация, используемая приложением, редко имеет единый уровень конфиденциальности. Более эффективно классифицировать информацию по группам внутри актива.

Пример — Информационный актив может состоять из десятков таблиц, где некоторые таблицы могут содержать конфиденциальную информацию.

Список требований безопасности в этом компоненте должен быть достаточно детализированным, чтобы его можно было эффективно использовать для планирования, разработки и внедрения МОБП.

Организация должна определить свои руководящие принципы и рекомендации по разработке МОБП, так как может внедрить либо полный набор атрибутов МОБП, описанных в ИСО/МЭК 27034-5, либо ряд атрибутов или несколько их наборов; организация также может адаптировать их для собственных нужд или текущих требований к документации для управления безопасностью.

Несмотря на то, что организация определяет свои собственные рекомендации и руководящие принципы МОБП, эти принципы должны удовлетворять минимальным требованиям, установленным в ИСО/МЭК 27034-5.

Для обеспечения согласованности группа НСО должна разработать рекомендации и руководящие принципы МОБП и сделать их доступными для команды разработчиков МОБП во время первых итераций процесса менеджмента НСО. Со временем процесс менеджмента НСО позволит развивать рекомендации и руководящие принципы МОБП.

5.5.3 Компонент регулятивного контекста

5.5.3.1 Назначение

Данный компонент помогает определить риски безопасности, исходящие из регулятивного контекста организации, точнее — риски, вызванные с тем, что организация не соблюдает соответствующие законы и правила. Этот компонент предоставляет значения, которые следует использовать в атрибуте МОБП «Направленный на требования». Компонент регулятивного контекста позволяет внедрить утвержденный стандартизированный метод снижения рисков, связанных с каждым применимым законом или нормативным актом.

5.5.3.2 Описание

Регулятивный контекст представляет собой список и задокументированное описание законов и нормативных актов, которые могут оказать влияние на проекты приложений в любом из регионов, где организация осуществляет свою деятельность, то есть в странах или юрисдикциях, где приложение разрабатывается, развертывается или используется.

Этот список будет особенно полезен для определения того, какие законы и нормативные акты имеют отношение к тем или иным спецификациям приложений и сферам коммерческой деятельности. Для этого в список необходимо добавить дополнительную информацию.

5.5.3.3 Содержание

Регулятивный контекст должен предоставить:

a) список законов и нормативных актов, применимых в зависимости от региона, где организация будет использовать приложение;

b) список рисков, сопутствующих вышеупомянутым законам и нормативным актам и имеющих отношение к безопасности приложений;

c) список требований безопасности для снижения вышеуказанных рисков.

5.5.3.4 Рекомендации

Информацию для создания регулятивного компонента НСО необходимо получать путем анализа рисков информационной безопасности. Организациям, которые провели анализ рисков информационной безопасности в соответствии с руководящими принципами ИСО/МЭК 27001:2013 и процессом менеджмента рисков, приведенным в ИСО/МЭК 27005:2011, потребуются минимальные усилия для создания этого компонента.

Список требований безопасности в этом компоненте должен быть достаточно детализированным, чтобы его можно было эффективно использовать для планирования, разработки и внедрения МОБП.

Организация должна уделить особое внимание созданию полного и точного списка законов и нормативных актов, применимых в зависимости от региона, где организация будет использовать приложения, и, возможно, даже выделить на это значительные ресурсы. Законы и нормативные акты будут применяться во всех странах, где создается проект приложения, проводится разработка, приобретение и развертывание приложения, где оно используется или эксплуатируется.

Сложная архитектура, например, в распределенных или облачных приложениях, может усугубить эту проблему. В распределенной архитектуре компоненты пользовательского интерфейса, обработки и хранения данных могут физически находиться в разных странах и подчиняться различным законам.

Поэтому организация должна:

a) разрешать возможные конфликты, связанные с большим количеством законов и обязательных требований;

b) отображать юридические требования в МОБП, с привлечением экспертов по правовым вопросам.

Описание этого процесса выходит за рамки настоящего стандарта.

Примечание — Эксперты по правовым вопросам будут выступать в качестве экспертов в предметных областях в процессах «Внедрение НСО» и «Мониторинг и оценка НСО» (подпункты 5.4.5.3 и 5.4.6.3).

5.5.4 Компонент технологического контекста

5.5.4.1 Назначение

Данный компонент помогает определить риски безопасности, исходящие от технологической инфраструктуры организации. Он предоставляет значения, которые следует использовать в атрибуте МОБП «Направленный на требования». Данный компонент предоставляет информацию о том, какие ИТ[1)]-компоненты могут использоваться для поддержки МОБП, требующих подобной поддержки.

5.5.4.2 Описание

Технологический контекст — это задокументированные ИТ-компоненты организации (например, физические компоненты, приложения, услуги) и лучшие методы работы и правила организации, которые применяются при использовании этих компонентов.

5.5.4.3 Содержание

Технологический контекст должен предоставить:

a) список ИТ-компонентов организации, которые имеют отношение к безопасности приложений;

b) перечень рисков, которые влекут за собой вышеупомянутые ИТ-компоненты организации;

c) список требований безопасности для снижения вышеуказанных рисков.

5.5.4.4 Рекомендации

Информацию для создания этого компонента НСО необходимо получать из технологической архитектуры организации путем анализа рисков информационной безопасности. Организациям, которые провели анализ рисков информационной безопасности в соответствии с руководящими принципами ИСО/МЭК 27001:2013 и процессом менеджмента рисков, предлагаемым в ИСО/МЭК 27005:2011, потребуются минимальные усилия для создания этого компонента.

Список требований безопасности в этом компоненте должен быть достаточно детализированным, чтобы его можно было эффективно использовать для планирования, проектирования и внедрения МОБП.

5.5.5 Репозиторий спецификаций приложений

5.5.5.1 Назначение

Данный компонент помогает определить риски безопасности, вытекающие из спецификаций приложений организации, а также снизить риск неправильного внедрения и (или) использования этих спецификаций. Он предоставляет значения, которые следует использовать в атрибуте МОБП «Направленный на требования».

5.5.5.2 Описание

Репозиторий спецификаций приложений представляет собой документацию об общих функциональных требованиях организации к ИТ и соответствующих предварительно одобренных решениях. Оно должно содержать все спецификации, функциональные возможности и услуги, предоставляемые приложениями организации или входящими в них, включая в себя документацию и лучшие методы работы для внедрения, использования и верификации.

Предварительно одобренные решения обычно представляют собой процессы, продукты или библиотеки кодов, рекомендуемых или обязательных к использованию на практике согласно правилам, политикам или корпоративной архитектуре организации, в зависимости от среды. Подобные решения обычно являются зрелыми и постоянно совершенствуются. Преимущество интеграции МОБП с такими решениями, постоянно используемыми повторно, является очевидным фактом.

5.5.5.3 Содержание

Репозиторий спецификаций приложений должен предоставлять следующее:

a) список спецификаций всех приложений, предлагаемых организацией;

b) для каждой спецификации список процессов и лучших методов работы, утвержденных организацией, которые используются для внедрения, использования, обслуживания или верификации приложений;

c) перечень рисков, которые влекут за собой вышеупомянутые спецификации приложений организации;

d) список требований безопасности для снижения рисков.

5.5.5.4 Рекомендации

Информацию для создания данного компонента НСО необходимо получать из документации об архитектуре приложений организации и корпоративной архитектуре организации.

[1)] *Информационные технологии (ИТ).*

Часть информации можно получить путем анализа рисков информационной безопасности. Организациям, которые провели анализ рисков информационной безопасности в соответствии с руководящими принципами ИСО/МЭК 27001:2013 и процессом менеджмента рисков, предлагаемым в ИСО/МЭК 27005:2011, потребуются минимальные усилия для создания этого компонента.

Список требований безопасности в этом компоненте должен быть достаточно детализированным, чтобы его можно было эффективно использовать для планирования, проектирования и внедрения МОБП.

Пример — Организация использует приложение под названием «Служба передачи файлов M012» и желает, чтобы все будущие проекты приложений также использовали эту службу для безопасной передачи документов между приложениями. Поэтому организация должна зарегистрировать эту службу в репозитории спецификаций приложений и указать там соответствующую информацию, например:

a) спецификация приложения является «передачей документов внешним по отношению к приложению и внутренним по отношению к организации субъектам»;

b) «процессы и лучшие методы работы» подразумевают, что «документы должны всегда, когда это возможно, передаваться с использованием «Службы передачи файлов M012», как указано в записи в технологическом контексте в НСО организации;

c) в список рисков входит «нарушение конфиденциальности документов, передаваемых между приложениями»;

d) список требований безопасности включает в себя «надежное шифрование файлов при передаче между конечными точками» и «аутентификацию на стороне сервера и клиента».

Затем, в ходе процесса менеджмента НСО, организация должна разработать МОБП, которое соответствовало бы требованиям безопасности, предписывая обязательное использование «Службы передачи файлов M012». В любом проекте приложения, где требуется функция передачи документов, должна использоваться именно та спецификация приложения, которая будет применять эти МОБП в проекте приложения.

5.5.6 Список ролей, обязанностей и квалификаций

5.5.6.1 Назначение

Данный компонент помогает определить риски безопасности, исходящие от сотрудников, работающих с приложениями организации. Благодаря этому компоненту обеспечивается то, что критически важные роли для всех процессов назначены, все обязанности распределены, предотвращены конфликты интересов, а сотрудники, назначенные на данные роли, имеют достаточную профессиональную квалификацию.

5.5.6.2 Описание

Список ролей, обязанностей и квалификаций — это документы, где описаны роли, обязанности и квалификация всех участников, работающих с приложениями организации.

5.5.6.3 Содержание

Список ролей, обязанностей и квалификаций должен включать в себя:

a) список всех ролей, связанных с приложениями организации;

Пример — В список входят: оператор приложения, архитектор приложений, архитектор безопасности, технологический архитектор, менеджер проектов, директор по информационной безопасности, владелец приложений, разработчики, директора, команда поддержки ИТ-инфраструктуры, преподаватели, поставщик, заинтересованные стороны, менеджер по информационной безопасности, специалисты по нормативно-правовым вопросам, тестировщики, пользователи;

b) список обязанностей, входящих в вышеуказанные роли;

c) список необходимых квалификаций для выполнения вышеупомянутых обязанностей.

5.5.6.4 Рекомендации

Информацию для создания данного компонента могут предоставить отдел кадров организации и ее бизнес-архитектура.

Список квалификаций в этом компоненте должен быть достаточно детализированным, чтобы его можно было эффективно использовать для планирования, разработки и внедрения МОБП.

5.5.7 Библиотека мер обеспечения безопасности приложений организации

5.5.7.1 Назначение

Компонент библиотеки МОБП используется для организации МОБП в соответствии с уровнями доверия приложений, к которым они относятся, чтобы упростить передачу МОБП и выбор соответствующих МОБП в ходе проекта приложения.

5.5.7.2 Описание

Библиотека МОБП — это репозиторий доступных организации МОБП. Каждая МОБП в репозитории связана с одним или несколькими уровнями доверия приложений.

5.5.7.3 Содержание

Библиотека МОБП должна предоставить следующие списки:

a) список уровней доверия приложений, используемых в организации, в том числе их идентификатор, название и описание;

b) список МОБП, назначенных каждому из уровней доверия приложения;

c) иерархический список всех МОБП, используемых в НСО.

5.5.7.4 Рекомендации

В процессе создания библиотеки МОБП организация должна использовать в качестве источника следующие данные:

a) рекомендуемые меры обеспечения безопасности согласно предыдущим аудиторским проверкам;

b) меры, разработанные по результатам оценки рисков;

c) меры, входящие в распространенные библиотеки, такие как ИСО/МЭК 27002, ИСО/МЭК 15408 и NIST SP 800-53;

d) меры, разработанные и предоставленные третьими сторонами, такими как поставщики, сообщества или другие организации.

В проектах могут применяться дополнительные подходы, специфические для системы, с учетом правил организации. Если меры были получены из других источников, то необходимо идентифицировать этот источник, чтобы организация могла отслеживать их изменения.

Группа НСО несет ответственность за создание библиотеки МОБП, удовлетворяющей конкретным требованиям и приоритетам в области обеспечения безопасности организации.

Ориентированный на приложения подход, приведенный в настоящем стандарте, позволяет достичь требуемой цели с помощью анализа новых или существующих приложений организации, определения связанных с ними рисков и требований безопасности, а также внедрения МОБП, отвечающих этим требованиям в соответствии с приоритетами, расставленными согласно рискам.

В качестве предварительной подготовки к данному процессу группа НСО должна внедрить необходимые компоненты НСО в первых итерациях процесса менеджмента НСО.

Пример 1 — Для определения рисков и приоритетов необходимо предоставить список информационных активов организации и их уровень конфиденциальности в компоненте бизнес-контекста НСО (подпункт 5.5.2.3).

Все задействованные компоненты НСО (бизнес-контекст, регулятивный и технологический контексты, список ролей, обязанностей и квалификаций и репозиторий спецификаций приложений) должны учитываться при анализе рисков для того, чтобы выработать требования безопасности, используемые для разработки МОБП.

Поскольку МОБП связаны с требованиями безопасности, изменение требований безопасности может повлечь за собой изменения во всех связанных МОБП.

Используя необходимые исходные данные, группа НСО определяет в ходе процесса «Проектирование НСО», какие приложения следует проанализировать в следующей итерации процесса менеджмента НСО. Некоторые организации отдают приоритет приложениям, которые используют информационные активы с высоким уровнем конфиденциальности.

Группа НСО должна выбрать те МОБП для внедрения в каждое из приложений, которые соответствуют требованиям безопасности приложений. Затем группа НСО должна выполнить процесс «Внедрение НСО» для данных МОБП. Рекомендации по внедрению МОБП приведены в 5.5.8.3.

В результате определяется набор МОБП, которые группа НСО должна добавить в библиотеку МОБП для их использования в проектах приложений.

МОБП могут быть добавлены в библиотеку МОБП тремя способами:

a) если набор МОБП уже имеет определенный уровень доверия приложения в библиотеке, то в этом случае в библиотеку ничего не добавляется — существующие МОБП просто обновляются;

b) если определенный уровень доверия приложения близко соответствует набору МОБП, то в этом случае библиотеку можно дополнить МОБП из набора;

c) создается новый уровень доверия приложения в библиотеке из набора МОБП.

Пример 2 — Организация выполняет этот процесс впервые. Библиотека МОБП пуста. Группа НСО решила включить в библиотеку МОБП новый набор МОБП в качестве нового уровня доверия приложения. Этот уровень доверия приложения обозначается как «клиент-серверное приложение С2 без доступа в Интернет», где «С2» — это уровень конфиденциальности информационных активов приложения на шкале от С1 до С4 (С4 — наиболее конфиденциальные, а С1 — наименее конфиденциальные). Этот уровень доверия приложения будет использоваться для всех аналогичных приложений, использующих информационные ресурсы С1 или С2.

Пример 3 — Та же организация снова выполняет данный процесс для другого приложения, очень похожего на приложение из примера 2, за исключением того, что оно использует некоторые активы уровня конфиденциальности С3 и имеет несколько дополнительных мер обеспечения безопасности. Поскольку новый набор МОБП очень похож на существующий уровень доверия приложения, группа НСО принимает решение обновить существующий уровень доверия приложения и переименовать его в «клиент-серверное приложение С3 без доступа в Интернет». Этот уровень доверия приложения будет использоваться для всех аналогичных приложений, использующих информационные ресурсы С1, С2 или С3. Объяснить это решение можно тем, что дополнительные затраты на использование «слишком большого количества» мер обеспечения безопасности приложений уровня конфиденциальности С1 и С2 более чем оправдают себя за счет огромной эффективности повторного использования существующего уровня доверия приложения.

Пример 4 — Та же организация выполняет данный процесс для нового проекта приложения, использующего информацию уровня конфиденциальности С2, но в качестве интернет-сервиса. Набор МОБП, внедренных в данное приложение, значительно отличается (50 % новых МОБП) от имеющихся в библиотеке МОБП. Группа НСО решает создать совершенно новый уровень доверия приложения в библиотеке и называет его «веб-приложение С2, имеющее доступ в Интернет». Поскольку 50 % МОБП используются повторно, организация по-прежнему выигрывает от повышения эффективности.

Пример 5 — Та же организация снова выполняет данный процесс для нового приложения, которое похоже на приложение из примера 2, за исключением того, что оно в основном использует активы уровня конфиденциальности С4, которые считаются критически важными для организации и к которым предъявляются особенно строгие нормативные требования, причем соблюдение этих требований тщательно проверяется. Набор МОБП, внедренных в это приложение, значительно отличается от любого уже существующего уровня доверия приложения в библиотеке МОБП: в него входит 70 % новых МОБП, большинство из которых — это мониторинг и контроль учетности на этапе использования жизненного цикла приложения, поэтому внедрять их достаточно дорого. Группа НСО решает создать совершенно новый уровень доверия приложения в библиотеке МОБП и называет его «клиент-серверное приложение С4 без доступа в Интернет». Этот уровень доверия приложения будет использоваться для всех похожих приложений, использующих информационные активы уровня конфиденциальности С4, но только для них, поскольку данный уровень конфиденциальности влечет за собой огромные затраты на эксплуатацию приложения. Поскольку 30 % МОБП используются повторно, организация по-прежнему выигрывает от повышения эффективности.

Пример 6 — Организация разработала внутреннее приложение критической важности под названием «Хранение», которое сделали настолько безопасным, насколько это возможно. В ходе нового критически важного проекта приложения владелец приложения заявляет, что хочет сделать так, чтобы у него был такой же уровень доверия приложения, как у приложения «Хранение». Группа НСО решает выполнить вышеуказанный процесс, оставив приоритет за приложением «Хранение». В результате уровень доверия приложения был назван «Такой же, как у Хранения». Затем группа НСО выполняет описанный выше процесс для нового приложения и определяет, что требования безопасности к нему действительно покрываются МОБП из уровня доверия приложения «Такой же, как у Хранения» в более чем достаточной степени. Команда разработчиков использует МОБП из этого уровня доверия приложения для нового приложения, и владелец приложения удовлетворен тем, что у его приложения уровень доверия приложения «Такой же, как у Хранения». Кроме того, снижается стоимость применения мер безопасности для нового приложения, потому что большая их часть уже используется в проекте «Хранение».

Как показано в предыдущих примерах и определено в ИСО/МЭК 27034-1, уровень доверия приложения — это обозначение (метка), которое присваивается набору МОБП, отвечающему требованиям безопасности одного или нескольких приложений, и, таким образом, определяющее уровень доверия приложения организации приложению, этим и объясняется название уровня доверия приложения.

Для данного обозначения не существует определенной номенклатуры, и отсутствуют требования для определения последовательности уровней доверия приложений.

Примечание 1 — В ИСО/МЭК 27034-1:2011 на рисунке 5 приведен пример уровней доверия приложений со значениями от 0 до 5.

При интеграции мер безопасности ИБ сторонних организаций необходимо сопоставить данные сторонних поставщиков со своими данными.

Пример 7 — Следуя рекомендации команды разработчиков МОБП, организация решает приобрести МОБП у стороннего поставщика, чтобы можно было проводить различные виды тестирования безопасности своих собственных приложений. Естественно, приобретенные у сторонних поставщиков МОБП не предназначены для библиотеки МОБП данной организации, поэтому их рекомендуемые уровни доверия приложений не сходятся. К счастью, сторонние МОБП экспортировались на открытом и мобильном языке обмена для МОБП, рекомендованном в ИСО/МЭК 27034-5, поэтому в определении МОБП содержатся уровни доверия приложений поставщика. Организация может сравнить уровни доверия приложений со своими и с легкостью сопоставить их, что позволит интегрировать МОБП в собственную библиотеку МОБП организации.

Примечание 2 — В ИСО/МЭК 27034-6 содержится более подробный пример интеграции сторонних МОБП.

Пример 8 — В Приложении В приводится краткое описание реального проекта по внедрению НСО в организации большого размера. Для реализации этого проекта использовался рабочий процесс, разработанный командой разработчиков специально для данной организации. Приведенный процесс является примером, поэтому данный процесс внедрения НСО не является обязательным для всех организаций.

5.5.8 Меры обеспечения безопасности приложений

5.5.8.1 Назначение

В данном компоненте описываются меры обеспечения безопасности приложения, чтобы облегчить их утверждение, обслуживание, использование, верификацию и передачу.

5.5.8.2 Содержание

ИСО/МЭК 27034-1:2011 содержит общую информацию о мерах обеспечения безопасности приложений (МОБП) и описывает данные, содержащиеся в МОБП. Организация может внедрять МОБП, используя описательный или другой нестандартный подход, выполняющий минимальные рекомендации, приведенные в ИСО/МЭК 27034-1:2011 (подпункт 8.1.2.6.5).

5.5.8.3 Рекомендации

Меры обеспечения безопасности приложений содержатся в библиотеке мер обеспечения безопасности приложений.

МОБП предназначены для того, чтобы формально описать все меры обеспечения безопасности, которые организация планирует использовать на всех этапах жизненного цикла любого из своих приложений.

Другие компоненты НСО, приведенные в настоящем стандарте, предоставляют собой наборы разрешенных значений для атрибутов, упомянутых в ИСО/МЭК 27034-1:2011 (подпункты 8.1.2.6.5.3 и 8.1.2.6.5.4) и ИСО/МЭК 27034-5 (подраздел 5.2):

a) «направленный на требования» (подпункты 5.5.2.3, 5.5.3.3, 5.5.4.3 и 5.5.5.3);

b) требуемые роли, обязанности и квалификации (подпункт 5.5.6.3);

c) «когда» (подпункт 5.5.9.3).

В ИСО/МЭК 27034-5 и ИСО/МЭК 27034-5-1 приведены более подробные описания структуры и типов всех элементов данных МОБП. Организации могут использовать эту структуру для создания совместимых МОБП, которые можно передавать другим организациям.

Кроме того, данная структура предоставляет наборы данных, которые помогут организации сопоставлять данные МОБП и позволят использовать их в процессах, таких как управление изменениями, управление соответствием и рисками.

В ИСО/МЭК 27034-6 приведены примеры МОБП, созданных с использованием этой структуры данных.

Необходимо четко определить роли лиц, участвующих в мероприятиях по обеспечению безопасности и проверочных измерениях МОБП, а также задокументировать их наряду с другими ролями лиц, принимающих участие в жизненном цикле приложений организации. Следует четко определить обязанности, например с помощью диаграмм RACI.

Необходимо удостовериться, что сотрудники, участвующие в мероприятиях по обеспечению безопасности и проверочных измерениях, обладают необходимой квалификацией.

Наряду с другими элементами НСО, организация должна создавать, анализировать и улучшать МОБП с помощью процессов менеджмента НСО, описанных в 5.4.4, 5.4.5, 5.4.6 и 5.4.7.

В ходе процесса «Проектирование НСО» группа НСО должна выбрать, какие МОБП будут разрабатываться (т. е. создаваться или поддерживаться) в рамках текущего цикла процесса менеджмента НСО, в соответствии с текущими приоритетами организации. При выборе МОБП приоритеты чаще всего устанавливаются в соответствии с текущими рисками, с которыми сталкивается организация, и насущными потребностями проектов приложений.

Затем группа НСО должна выполнить процесс «Внедрение НСО». Для каждого из выбранных МОБП или группы связанных МОБП следует:

a) назначить группу разработчиков МОБП, состав которой зависит от набора умений, необходимых для разработки приемлемого решения (например, «меры по обеспечению безопасности» и «проверочные мероприятия») для удовлетворения конкретных «требований безопасности» МОБП на «рекомендуемом уровне доверия приложения».

Примечание — Группа НСО должна выделять достаточное количество ресурсов и сотрудников для разработки, проверки и улучшения элементов НСО, особенно экспертов в предметной области, подходящих для конкретной МОБП.

Пример — Экспертами в предметной области могут являться эксперты в юриспруденции, судебные эксперты, технические специалисты, эксперты по криптографии, специалисты по режиму конфиденциальности;

b) донести до ответственных лиц задачи по обеспечению безопасности приложений и дать рекомендации команде разработчиков, какие действия необходимо выполнить для соответствия требованиям безопасности и рекомендуемым уровням доверия приложений для МОБП;

c) предоставить достаточное количество ресурсов команде разработчиков, в том числе времени, финансовых ресурсов, средств управления проектами, инструментальных средств, документации, знаний и технических ресурсов, таких как лаборатории для разработки;

d) позволить команде разработчиков спроектировать, разработать и внедрить МОБП, что обычно делается с помощью проектных мероприятий;

e) утвердить проект, разработанную МОБП и включить ее в библиотеку МОБП;

f) обеспечить достаточный уровень подготовки действующих субъектов, определенный командой разработчиков, в соответствии с ролями, обязанностями и квалификацией, необходимыми как для деятельности по обеспечению безопасности, так и для верификации МОБП.

В ходе разработки и внедрения МОБП команда разработчиков должна найти приемлемое решение для удовлетворения требований безопасности на рекомендованных уровнях доверия приложений, определенных группой НСО. Команда разработчиков должна:

a) получить полное представление о требованиях безопасности, определенных группой НСО, их истории и контексте. Это подразумевает проведение совещаний с различными подразделениями и лицами, которые выдвинули требование, например с командой проекта приложения, а также ознакомление с нормативной документацией по проекту приложения. Важно понимать значение рекомендуемого(ых) уровня(ей) доверия приложений МОБП. Эта информация содержится в библиотеке МОБП;

b) составить список существующих решений. В этот список могут входить поиск в библиотеке МОБП существующих МОБП, отвечающих тем же или аналогичным требованиям безопасности, поиск готовых МОБП вне организации или поиск готовых мер, еще не описанных в структуре данных МОБП;

c) в достаточной мере понять текущие технологический, регулятивный и бизнес-контексты организации, применимые к требованию безопасности, чтобы исключить решения, не соответствующие контекстам организации или трудно интегрируемые в них;

d) изучить различные решения и выбрать те, которые наилучшим образом минимизирует риски безопасности, определенные в требованиях безопасности и контексте организации;

e) полностью изучить рекомендации и руководящие принципы организации для разрабатываемой ею МОБП. Эта информация должна содержаться в компонентах НСО. Примеры представлены ниже.

Примеры

1 Рекомендации и руководящие принципы МОБП содержат атрибуты МОБП, области значений, правила, номенклатуру и зависимости для каждого атрибута.

2 Регулятивный, технологический контексты и бизнес-контекст формируют требования, на которые следует ссылаться в атрибуте МОБП «Направленный на требования».

3 Список ролей, обязанностей и квалификаций содержит значения для ролей и обязанностей в описании мер по обеспечению безопасности и верификации МОБП.

4 Эталонная модель жизненного цикла безопасности приложения предоставляет значения для атрибута «когда» в описании мероприятий по обеспечению безопасности и верификации МОБП;

f) задокументировать решение в виде МОБП, предоставляя значения для каждой МОБП в соответствии с рекомендациями и руководящими требованиями организации.

Новой МОБП может быть одна из нижеследующих:

a) совершенно новая МОБП;

b) доработанная существующая МОБП, тогда новая МОБП может быть:

1) новым экземпляром существующей МОБП для другого требования;

2) более точной реализацией родительской МОБП;

3) новой версией существующей МОБП с дополненным или исправленным содержимым.

Новую МОБП необходимо надлежащим образом занести в библиотеку МОБП, чтобы облегчить ее повторное использование. Это означает, что она должна быть связана с соответствующими родительскими МОБП через атрибут «родитель». Кроме того, новую МОБП можно внести в библиотеку в качестве родительской для других МОБП, которые также следует изменить, чтобы отразить их взаимоотношения с родительской мерой (средством).

Примечание — По мере усложнения библиотеки МОБП организации следует подумать об использовании технологического решения для управления библиотекой.

Во многих случаях, особенно когда организация находится на ранних этапах внедрения НСО, работа команды разработчиков состоит в основном в том, чтобы вписать существующие МОБП в структуру данных МОБП. Эта структура позволяет добавлять ссылки на задокументированный проект существующей меры обеспечения безопасности приложения или прикреплять такие документы к МОБП.

Со временем все больше организаций будут записывать меры обеспечения безопасности в шаблоны МОБП и выкладывать их в общий доступ, поэтому командам разработчиков станет проще приобретать МОБП у других организаций и адаптировать их к требованиям и условиям своей организации. В таких случаях рекомендуется создавать новую адаптированную версию приобретенной МОБП, сохраняя оригинальную версию в качестве справочного материала.

Каждая МОБП должна быть полностью завершена, т. е. команда разработчиков должна предоставить значения для всех атрибутов в шаблоне, даже если это значение является неполным или пока неизвестно. Это дает больше информации, чем пустой атрибут, поскольку указывает на то, что атрибут действительно рассматривался и было принято решение о присвоении ему значения, даже если это значение еще неизвестно.

5.5.9 Эталонная модель жизненного цикла безопасности приложений

5.5.9.1 Назначение

Назначение данного компонента заключается в том, чтобы:

a) помочь организации понять, когда МОБП применяются в жизненном цикле приложения (т. е. предоставить набор допустимых значений для атрибута МОБП «когда»);

b) предоставить информацию о ролях, задействованных в выполнении мероприятий или задач МОБП;

c) помочь организации проверить каждый этап жизненного цикла приложений, определив мероприятия и участников, потенциально вовлеченных в обеспечение безопасности приложений;

d) содействовать организации в нахождении правильного подхода к решению проблем безопасности на всех этапах жизненного цикла приложений;

e) помочь организации минимизировать затраты и негативный эффект от внедрения методов ИСО/МЭК 27034 в проекты приложений, сохраняя существующий жизненный цикл приложений;

f) облегчить общение между командами, работающими в разных областях знаний;

g) предоставить организации стандартную модель для согласования МОБП между группами разработчиков приложений, несмотря на различные модели жизненного цикла приложений;

h) предоставить организациям стандартную модель для совместного использования МОБП, независимо от различных моделей жизненного цикла приложений.

5.5.9.2 Описание

Данный компонент предоставляет эталонную модель жизненного цикла безопасности приложения (см. рисунок 3), которая используется для сравнения с собственными моделями организации. Он предоставляет стандартизированный список областей деятельности, мероприятий и ролей, связанных с управлением, разработкой программных средств, ИТ-инфраструктурой и аудитом приложений. Этот компонент выступает в качестве эталонной модели жизненного цикла безопасности приложений, ко-

торая помогает организации проводить идентификацию и обмениваться данными в ходе жизненного цикла приложения, для которого внедряются МОБП.

Эталонная модель разделена горизонтально на два основных этапа: этап подготовки к работе, во время которого осуществляются мероприятия по приемке и развертыванию приложения, и этап эксплуатации, во время которого выполняются послереализационные мероприятия.

Этапы подготовки к работе и эксплуатации можно разделить на следующие стадии:

a) подготовка к работе состоит из трех стадий: подготовки, реализации и ввода в эксплуатацию;

b) эксплуатация состоит из трех стадий: эксплуатации и сопровождения, архивирования, уничтожения.

Эталонная модель разделена вертикально на четыре основных уровня:

a) менеджмент приложений: этот уровень включает в себя мероприятия из сферы корпоративного управления, такие как менеджмент проектов и менеджмент эксплуатации приложений. Эти мероприятия обычно выполняются в рамках процессов, определенных в системе менеджмента информационной безопасности организации;

b) подготовка к работе и эксплуатация приложения: этот уровень включает в себя мероприятия, связанные с подготовкой к работе и использованием самого приложения. Эти мероприятия обычно выполняются в рамках процессов, рекомендованных такими стандартами, как семейство ИСО/МЭК 15026, ИСО/МЭК 15288, ИСО/МЭК 12207 и ИСО/МЭК 21827;

c) менеджмент инфраструктуры: этот уровень состоит из мероприятий, связанных менеджментом инфраструктуры ИТ-услуг, которая поддерживает использование приложений в организации. Эти мероприятия обычно выполняются в рамках процессов, рекомендованных ИСО/МЭК ТО 20000-4 и руководством по управлению ИТ-услугами (ITIL[1]);

d) аудит приложений: этот уровень включает в себя мероприятия, связанные с контролем и верификацией. Эти мероприятия обычно выполняются в рамках процессов, рекомендованных такими стандартами, как ИСО/МЭК 15288, ИСО/МЭК 12207, и документами, содержащими описание практических приемов индустрии, например COBIT[2].

Рисунок 3 — Графическое высокоуровневое представление эталонной модели жизненного цикла безопасности приложений

[1] *Библиотека инфраструктуры информационных технологий (ITIL).*

[2] *Задачи управления для информационных и смежных технологий (COBIT).*

5.5.9.3 Содержание

5.5.9.3.1 Роли

Эталонная модель жизненного цикла безопасности приложений должна предоставлять список ролей всех действующих субъектов, выполняющих действия в рамках эталонной модели жизненного цикла безопасности приложений, чтобы организация могла по единому принципу идентифицировать и доводить до ответственных лиц роли, обязанности и необходимые квалификации, определяя набор допустимых значений для атрибутов МОБП «Роли», «Обязанности» и «Требуемая квалификация».

Для определения набора допустимых значений настоятельно рекомендуется использование организацией стандартизированного списка ролей из ИСО/МЭК 27034-5. Это позволяет различным проектным командам использовать МОБП совместно внутри организации или с другими организациями.

5.5.9.3.2 Мероприятия

Эталонная модель жизненного цикла безопасности приложения должна предоставлять подробный список мероприятий в виде набора допустимых значений для атрибута МОБП «Когда». Организация должна использовать стандартизированный перечень мероприятий, приведенный в ИСО/МЭК 27034-5-1. Это позволяет различным проектным командам использовать МОБП совместно внутри организации или с другими организациями.

Описания мероприятий, выполняемых на разных этапах жизненного цикла безопасности приложения и изображенных на рисунке 3, приведены ниже.

5.5.9.3.2.1 Менеджмент приложений

Мероприятия по менеджменту приложений выполняются менеджерами проектов и менеджерами организаций на этапах подготовки к работе приложений.

Подобные мероприятия обычно выполняются в рамках общеорганизационных процессов. К ним относятся процессы разработки программных средств из группы процессов проекта, приведенные в ИСО/МЭК 12207, такие как процесс менеджмента людскими ресурсами, процесс планирования проекта, процесс оценки и контроля проекта, процесс принятия решений.

Чтобы более точно определить, когда следует выполнять мероприятия по обеспечению безопасности, организация может разбить эту группу мероприятий на такие подгруппы, как инициация, планирование, выполнение, мониторинг и контроль, а также закрытие.

5.5.9.3.2.2 Менеджмент эксплуатации приложений

Мероприятия менеджмента эксплуатации приложений связаны с менеджментом и использованием приложения на этапе эксплуатации.

Подобные мероприятия обычно выполняются в рамках общеорганизационных процессов организации. К ним относятся процессы разработки программных средств из ИСО/МЭК 12207, такие как процесс принятия решений и процесс менеджмента информации.

Обычно за приложение отвечает его владелец, который может разделить часть своей ответственности с другими действующими субъектами, такими как руководители пользователей.

Внесение изменений в приложение на этапах эксплуатации, например изменений, связанных с новыми нормативными требованиями или угрозами, должно инициироваться владельцем приложений, отвечающим за обеспечение уверенности в том, что приложения надлежащим образом и постоянно учитывают меняющиеся потребности организации в безопасности.

Владелец приложения создает систему менеджмента информационной безопасности организации с помощью этих процессов. Он также должен предоставить необходимые свидетельства и обеспечить доверие к рассмотрению вопросов корпоративного управления проектами приложений.

Чтобы более точно определить, когда следует выполнять мероприятия по обеспечению безопасности приложений, организация может разбить группу мероприятий на такие подгруппы, как инициация, планирование, выполнение, мониторинг и контроль, а также закрытие.

5.5.9.3.2.3 Подготовка

На этапе подготовки к работе команда обеспечения выполняет предварительные или подготовительные мероприятия. Подобные мероприятия обычно выполняются в рамках общеорганизационных процессов. К ним относятся процессы разработки программных средств из ИСО/МЭК 12207, такие как процесс принятия решений (пункт 6.3.3) и процесс менеджмента информации (пункт 6.3.6).

Чтобы более точно определить, когда следует выполнять мероприятия по обеспечению безопасности, организация может разбить эту группу мероприятий на такие подгруппы, как инициация и планирование.

5.5.9.3.2.4 Аутсорсинг

На этапе реализации команда, занимающаяся подготовкой к работе, осуществляет мероприятия, связанные с реализацией программных средств. Если некоторые мероприятия по реализации программных средств организация осуществляет через аутсорсинг, то для достижения целевого уровня доверия приложения, возможно, потребуется добавить к мероприятиям по реализации специальные МОБП. Поэтому эталонная модель жизненного цикла безопасности приложений должна включать в себя определенную сферу деятельности для аутсорсинга.

Подобные мероприятия обычно выполняются в рамках общеорганизационных процессов. К ним относятся процессы проектирования программных средств из ИСО/МЭК 12207, в том числе процесс приобретения, процесс менеджмента документации программных средств, процесс менеджмента конфигурации программных средств и процесс менеджмента рисков.

Чтобы более точно определить, когда следует выполнять мероприятия по обеспечению безопасности, организация может разбить эту группу мероприятий на такие подгруппы, как реализация и ввод в эксплуатацию.

5.5.9.3.2.5 Разработка

На этапе реализации группа, занимающаяся подготовкой к работе, осуществляет мероприятия, связанные с внедрением программных средств. Если организация осуществляет внедрение некоторых мероприятий своими силами, то МОБП, добавленные к мероприятиям по внедрению могут отличаться от тех, которые добавляются в случае приобретения или аутсорсинга внедрения компонентов приложений. Поэтому эталонная модель жизненного цикла безопасности приложений включает в себя определенную область мероприятий разработки с последующей реализацией программных средств силами организации.

Такие мероприятия обычно осуществляются как часть процессов в масштабах организации. Они включают в себя процессы проектирования программных средств из ИСО/МЭК 12207, такие как процесс менеджмента риска, проектирование на уровне архитектуры системы, процесс архитектурного проектирования программных средств, процесс детального проектирования программных средств, процесс создания программных средств, процесс менеджмента документации программных средств, процесс менеджмента конфигурации программных средств, процесс верификации программных средств, процесс утверждения программных средств, процесс проверки программных средств, процесс доменного проектирования и процесс менеджмента повторного использования активов.

Чтобы более точно определить, когда следует выполнять мероприятия по обеспечению безопасности, организация может разбить эту группу мероприятий на такие подгруппы, как начальная подготовка, проработка, создание и внедрение.

5.5.9.3.2.6 Приобретение

Группа, занимающаяся подготовкой к работе, может осуществлять мероприятия по приобретению с целью внешнего получения или приобретения продукта и (или) услуги, отвечающих потребностям организации. К этим мероприятиям могут добавляться специальные МОБП. Поэтому эталонная модель жизненного цикла безопасности приложений включает в себя определенную область мероприятий приобретения с последующей реализацией приобретенных компонентов приложений.

Такие мероприятия обычно осуществляются как часть процессов в масштабах организации. К ним относятся процессы проектирования программных средств из ИСО/МЭК 12207, такие как процесс приобретения, процесс менеджмента документации программных средств, процесс менеджмента конфигурации программных средств, процесс менеджмента риска и процесс реализации.

Чтобы более точно определить, когда следует выполнять мероприятия по обеспечению безопасности, организация может разбить эту группу мероприятий на такие подгруппы, как планирование и закрытие.

5.5.9.3.2.7 Ввод в эксплуатацию

На этапе ввода в эксплуатацию группа, занимающаяся подготовкой к работе, выполняет мероприятия с целью подготовки, конфигурирования, тестирования и развертывания приложения в среде эксплуатации, определяемой организацией. Подобные мероприятия обычно выполняются в рамках общеорганизационных процессов. К ним относятся процессы разработки программных средств из ИСО/МЭК 12207, такие как процесс менеджмента конфигурации программных средств, процесс системной интеграции и процесс проверки соответствия системы техническим условиям.

Чтобы более точно определить, когда следует выполнять мероприятия по обеспечению безопасности, организация может разбить эту группу мероприятий на такие подгруппы, как планирование, разработка и тестирование.

5.5.9.3.2.8 Эксплуатация

На этапе эксплуатации и сопровождения осуществляются мероприятия, связанные с фактическим использованием приложения в среде эксплуатации всеми пользователями, включая конечных пользователей. К подобным мероприятиям относятся управление доступом пользователей, протоколирование, мониторинг, обучение мерам безопасности и т. д.

С целью сопровождения программных средств и управления изменениями осуществляются другие мероприятия, в том числе обновление прикладного программного средства для выполнения меняющихся информационных требований, например, добавление новых функций и изменение формата данных. Сюда также относятся мероприятия по исправлению ошибок и адаптации программных средств к новым аппаратным устройствам.

Такие мероприятия обычно осуществляются как часть процессов в масштабах организации. К ним относятся процессы проектирования программных средств из ИСО/МЭК 12207, такие как процесс эксплуатации программных средств и процесс сопровождения программных средств.

Чтобы более точно определить, когда следует выполнять мероприятия по обеспечению безопасности, организация может разбить эту группу мероприятий на такие подгруппы, как эксплуатация и обслуживание.

5.5.9.3.2.9 Архивирование

Мероприятия по архивированию осуществляются группой, занимающейся эксплуатацией, в случае, когда приложение в его активном состоянии уже не используется. К таким мероприятиям относится архивирование всей информации приложения, включая архивирование всех инструментальных средств и процессов для обеспечения защиты и безопасного доступа к этой информации, если приложение больше уже не работает в своей среде эксплуатации.

Такие мероприятия обычно осуществляются как часть процессов в масштабах организации. К ним относятся процессы проектирования программных средств из ИСО/МЭК 12207, такие как процесс вывода программных средств из эксплуатации.

Чтобы более точно определить, когда следует выполнять мероприятия по обеспечению безопасности, организация может разбить эту группу мероприятий на такие подгруппы, как планирование, исполнение и верификация.

5.5.9.3.2.10 Уничтожение

Мероприятия по уничтожению связаны с безопасным разрушением всей информации приложений, в том числе данных пользователей, информации организации, журналов регистрации пользователей, параметров приложений и т. д.

Такие мероприятия обычно осуществляются как часть процессов в масштабах организации. К ним относятся процессы проектирования программных средств из ИСО/МЭК 12207, такие как процесс вывода программных средств из эксплуатации.

Чтобы более точно определить, когда следует выполнять мероприятия по обеспечению безопасности, организация может разбить эту группу мероприятий на такие подгруппы, как планирование, исполнение и верификация.

5.5.9.3.2.11 Менеджмент обеспечения инфраструктуры приложений

Эта сфера деятельности на этапе подготовки к работе включает в себя мероприятия, связанные с обеспечением и поддержанием безопасной технологической инфраструктуры в поддержку мероприятий, осуществляемых занимающейся подготовкой к работе группой. Сюда относятся услуги, средства, инструменты и активы информационно-коммуникационной технологии в среде разработки и различных видах среды тестирования.

Такие мероприятия обычно осуществляются как часть процессов в масштабах организации. К ним относятся процессы проектирования программных средств из ИСО/МЭК 12207, такие как процесс менеджмента инфраструктуры и процесс менеджмента конфигурации.

Чтобы более точно определить, когда следует выполнять мероприятия по обеспечению безопасности, организация может разбить эту группу мероприятий на такие подгруппы, как установка, эксплуатация, обслуживание, поддержка и архивирование.

5.5.9.3.2.12 Менеджмент инфраструктуры эксплуатации приложений

Эта сфера деятельности на этапе подготовки к работе включает в себя мероприятия, связанные с обеспечением и поддержанием безопасной технологической инфраструктуры для этапа эксплуатации жизненного цикла приложений. Сюда относятся также услуги, средства, инструменты и активы информационно-коммуникационной технологии в среде эксплуатации приложений.

На этапе эксплуатации также должны проводиться другие мероприятия для поддержания безопасной инфраструктуры, поддерживающей приложение. Поддержка инфраструктуры включает в себя техническое обслуживание систем и сетевых аппаратных средств, резервное копирование и восстановление, восстановление после бедствия и т. д.

Такие мероприятия обычно осуществляются как часть процессов в масштабах организации. К ним относятся процессы проектирования систем из ИСО/МЭК 15288, такие как процесс эксплуатации и процесс поддержки.

Чтобы более точно определить, когда следует выполнять мероприятия по обеспечению безопасности, организация может разбить эту группу мероприятий на такие подгруппы, как поддержка, эксплуатация, обслуживание и архивирование.

5.5.9.3.2.13 Вывод из эксплуатации

Мероприятия вывода из эксплуатации осуществляются с целью обеспечения уверенности в том, что вся информация, хранящаяся в системах, на серверах и других используемых приложениями технологических компонентах, безопасным образом удаляется. Это дает возможность утилизации или переработки этих компонентов без излишнего риска безопасности для организации.

Такие мероприятия обычно осуществляются как часть процессов в масштабах организации. Они включают в себя процессы проектирования систем из ИСО/МЭК 15288, такие как процесс вывода из эксплуатации.

Чтобы более точно определить, когда следует выполнять мероприятия по обеспечению безопасности, организация может разбить эту группу мероприятий на такие подгруппы, как планирование, исполнение и верификация.

5.5.9.3.2.14 Аудит подготовки приложений к работе

Мероприятия аудита осуществляются для всей деятельности, действующих субъектов, процессов, артефактов и компонентов приложений, используемых или создаваемых во время жизненного цикла приложений.

Эти мероприятия могут выполняться единожды или периодически, внутренними или внешними аудиторскими группами в зависимости от целевого уровня доверия приложения проекта приложения. Они обеспечивают владельцу приложения необходимое доверие и свидетельства того, что требования безопасности приложений выполняются, как ожидалось.

Мероприятия аудита, проводимые на этапе подготовки к работе, обычно отличаются от мероприятий аудита, осуществляемых на этапе эксплуатации. Организациям, разрабатывающим, но не эксплуатирующим приложения (таким как производители программных средств), может никогда не потребоваться проведение аудита приложений на этапе эксплуатации. Поэтому эталонная модель жизненного цикла безопасности приложений предоставляет определенную сферу для мероприятий аудита, проводимых на этапе подготовки к работе.

Такие мероприятия обычно осуществляются как часть процессов в масштабах организации. Они включают в себя процессы проектирования программных средств из ИСО/МЭК 12207, такие как процесс аудита программных средств.

Чтобы более точно определить, когда следует выполнять мероприятия по обеспечению безопасности, организация может разбить эту группу мероприятий на такие подгруппы, как планирование, приобретение, внедрение, поставка, обслуживание, мониторинг и оценка.

5.5.9.3.2.15 Аудит эксплуатации приложений

Мероприятия аудита, проводимые на этапе эксплуатации, обычно отличаются от мероприятий аудита, осуществляемых на этапе подготовки к работе. Организациям, только эксплуатирующим приобретенные приложения, может никогда не потребоваться проведение аудита приложений на этапе подготовки к работе. Поэтому эталонная модель жизненного цикла безопасности приложений предоставляет определенную сферу для мероприятий аудита, проводимых на этапе эксплуатации.

Такие мероприятия обычно осуществляются как часть процессов в масштабах организации. Они включают в себя процессы проектирования программных средств из ИСО/МЭК 12207, такие как процесс аудита программных средств.

Чтобы более точно определить, когда следует выполнять мероприятия по обеспечению безопасности, организация может разбить эту группу мероприятий на такие подгруппы, как планирование, приобретение, внедрение, поставка, сопровождение, мониторинг и оценка.

5.5.10 Модель жизненного цикла безопасности приложений

5.5.10.1 Назначение

Назначение данного компонента НСО состоит в том, чтобы:

a) помочь организации идентифицировать и официально задокументировать уже используемые ею модели жизненного цикла безопасности приложения;

b) помочь организации завершить при необходимости эти модели, используя эталонную модель жизненного цикла безопасности приложений, приведенную в настоящем стандарте (т. е. добавить уровни, этапы, мероприятия или участников);

c) облегчить передачу МОБП командам разработчиков приложений;

d) облегчить интеграцию МОБП с другими мероприятиями, уже выполняемыми командами разработчиков приложений.

5.5.10.2 Описание

Модель жизненного цикла безопасности приложения основана на модели жизненного цикла приложения, но используется для управления мероприятиями по обеспечению безопасности приложений. Она состоит из уровней, этапов и мероприятий.

5.5.10.3 Содержание

Данный компонент НСО необходим для того, чтобы задокументировать один или несколько уже используемых организацией жизненных циклов с помощью эталонной модели жизненного цикла безопасности приложений.

5.5.10.4 Рекомендации

Разные организации используют различные модели жизненного цикла. В организациях разные модели жизненного цикла зачастую используются разными группами разработчиков, в разных подразделениях и в разных проектах. Настоящий стандарт не предназначен для того, чтобы навязать стандартную модель жизненного цикла организациям или командам разработчиков приложений.

Поэтому МОБП, используемые мероприятия из стандартизированной эталонной модели жизненного цикла безопасности приложений НСО (см. 5.5.9), необходимо «адаптировать» перед передачей группам разработчиков приложений, чтобы их можно было интегрировать в привычную модель жизненного цикла. Процедура сравнения, предоставляемая в данном компоненте, используется именно для этого. Это может быть представлено в виде простой таблицы «перечисляемых типов», приведенной в ИСО/МЭК 27034-5-1, где добавляются столбцы для каждой из моделей жизненного цикла организации. В ИСО/МЭК 27034-6 этот метод описывается на примере «использования ЭМЖЦБП для облегчения внедрения МОБП различными группами разработчиков внутри организации».

Этапы обеспечения в моделях жизненного цикла безопасности приложений организации должны включать в себя все мероприятия по подготовке приложений организации. Этапы эксплуатации в моделях жизненного цикла безопасности приложений организации должны включать в себя все мероприятия по эксплуатации приложений организации.

Возможно, в модель жизненного цикла безопасности приложения необходимо будет добавить уровни, этапы, мероприятия или участников, чтобы все МОБП, необходимые для целевого уровня доверия приложения, можно было применять в полной мере в течение всего жизненного цикла приложения.

Для обеспечения безопасности разрабатываемых приложений может потребовать постоянное улучшение моделей жизненного цикла приложений организации, поддерживаемых в рамках процесса менеджмента НСО. Их обновляют исходя из результатов предыдущих аудитов и результатов оценки рисков, чтобы разрабатываемые приложения были максимально устойчивыми к атакам и не влекли за собой неприемлемых угроз безопасности.

При оценке и улучшении модели жизненного цикла безопасности приложений группа НСО и работающие с ней эксперты в данной области должны понимать, насколько большую роль играют определение, реализация, обслуживание и передача ответственным лицам модели жизненного цикла безопасности приложений для достижения бизнес-задач и обеспечения безопасности. Для этого необходимо организовать нормативные элементы, меры обеспечения безопасности приложения и мероприятия на протяжении всего жизненного цикла приложений.

Для оценки и улучшения модели жизненного цикла безопасности приложений необходимо учитывать следующие исходные данные:

a) эталонную модель жизненного цикла безопасности приложения, представленную в настоящем стандарте (пункт 5.5.9);

b) жизненные циклы приложений организации и процессы жизненного цикла;

c) методы разработки программных средств организации;

d) меры обеспечения безопасности приложений организации;

e) результаты оценки рисков безопасности приложений;

f) замечания разработчиков программных средств и пользователей организации, а также других заинтересованных сторон.

5.5.11 Процесс менеджмента безопасности приложений

5.5.11.1 Назначение

Процесс менеджмента безопасности приложений позволяет организации управлять безопасностью всех используемых ею приложений.

5.5.11.2 Описание

Процесс менеджмента безопасности приложений — это общий процесс менеджмента безопасности всех приложений, используемых организацией. Это специализация процесса менеджмента рисков, приведенного в ИСО/МЭК 27005.

5.5.11.3 Результаты

Результатом этого процесса в ходе проекта приложения являются:

a) определение требований и среды приложения;

b) оценка рисков информационной безопасности приложения;

c) определение требований безопасности приложения на базе оценки рисков, которые выражаются в виде целевого уровня доверия приложения;

d) обработка рисков начинается с выбора подходящих МОБП в соответствии с целевым уровнем доверия приложения;

e) устраняются риски информационной безопасности приложения с помощью выполнения мероприятий по обеспечению безопасности и проверочных измерений, определенных в рамках выбранных МОБП;

f) измеряется остаточный риск приложения с помощью определения фактического уровня доверия приложения в ходе процесса верификации приложения.

5.5.11.4 Мероприятия по внедрению

Таблица 15 — Диаграмма RACI для внедрения процесса менеджмента безопасности приложений

Мероприятия по внедрению	Владелец приложения	Команда разработчиков приложения	Аудитор
1) Выполнение этапа «Определение требований и среды приложения»	A	R	
2) Выполнение этапа «Оценка рисков безопасности приложения»	A	R	
3) Выполнение этапа «Создание и поддержка нормативной структуры приложения»		A/R	
4) Выполнение этапа «Обеспечение и эксплуатация приложения»		A/R	C
5) Выполнение этапа «Аудит безопасности приложения»	A	C	R

5.5.11.5 Мероприятия по верификации

Таблица 16 — Диаграмма RACI для верификации процесса менеджмента безопасности приложений

Мероприятия по верификации	Группа НСО	Владелец приложения	Команда разработчиков приложения	Аудитор
1) Подтверждение того, что этап «Определение требований и среды приложения» выполнен верно в ходе проекта приложения организации	A	C	C	R
2) Подтверждение того, что этап «Оценка рисков безопасности приложения» выполнен верно в ходе проекта приложения организации	A	C	C	R
3) Подтверждение того, что этап «Создание и поддержка нормативной структуры приложения» выполнен верно в ходе проекта приложения организации	A		C	R
4) Подтверждение того, что этап «Обеспечение и эксплуатация приложения» выполнен верно в ходе проекта приложения организации	A		C	R

Окончание таблицы 16

Мероприятия по верификации	Группа НСО	Владелец приложения	Команда разработчиков приложения	Аудитор
5) Подтверждение того, что этап «Аудит безопасности приложения» выполнен верно в ходе проекта приложения организации		A	C	R

5.5.11.6 Рекомендации

Обзор пяти этапов, упомянутых в 5.5.11.4, приведен в ИСО/МЭК 27034-1:2011 (разделы 7 и 8). Подробное описание процесса менеджмента безопасности приложений приведено в ИСО/МЭК 27034-3, и рекомендации по этому процессу представлены в настоящем стандарте.

Аудитор, ответственный за проведение верификации мероприятия 5 из таблицы 16, должен быть независимым от аудитора, который выполнял мероприятие 5 из таблицы 15. Необходимо подтвердить независимость аудитора по отношению к объекту аудита.

5.5.12 Процесс анализа рисков безопасности приложений

5.5.12.1 Назначение

Данный процесс позволяет идентифицировать и оценить риски безопасности приложений на протяжении всего жизненного цикла приложений, чтобы создать точный и воспроизводимый процесс анализа рисков безопасности приложений, а также инструменты анализа рисков, утвержденные организацией.

5.5.12.2 Описание

Процесс анализа рисков безопасности приложений — это процесс определения рисков всех приложений, используемых организацией. Это специализированная часть процесса менеджмента рисков, представленного в ИСО/МЭК 27005.

5.5.12.3 Содержание

Данный компонент НСО представляет собой документацию о процессах, мероприятиях и инструментальных средствах, одобренных организацией для проведения анализа рисков информационной безопасности в рамках области применения приложения.

Данный компонент НСО должен определять риски безопасности приложения, исходя из уязвимостей, угроз и воздействия бизнес-рисков, связанных с используемыми приложением активами (компонентами), а также расставлять приоритеты возникающих рисков.

5.5.12.4 Рекомендации

Организация должна выбрать или определить процесс анализа рисков безопасности приложений, который является адекватным для анализа рисков приложений. Не каждый процесс анализа рисков может подойти: большинство из процессов были разработаны для оценки рисков безопасности организации, поэтому сложно уменьшить их масштаб.

В ходе процесса анализа рисков необходимо обеспечение возможности управлять идентификацией рисков безопасности приложения в установленной области применения и с учетом активов (компонентов), используемых приложением. Следует также уделить внимание изучению среды эксплуатации, в которой приложение будет эксплуатироваться, чтобы определить, какие компоненты приложения уязвимы для конкретных угроз, и выяснить возможные последствия нарушения конфиденциальности, целостности и доступности этих компонентов.

Процесс анализа рисков безопасности приложений должен использоваться на этапе 2 ПМБП «Оценка рисков безопасности приложений», который приведен в ИСО/МЭК 27034-1:2011 (пункт 8.3.3). Таким образом, необходимо использовать в качестве исходных данных выходные данные этапа 1 ПМБП «Определение требований и среды приложения», такие как:

a) технологический, регулятивный контексты и бизнес-контекст приложения;

b) спецификации приложения.

Результатом выполнения процесса анализа рисков безопасности приложения должны быть следующие данные:

a) список угроз безопасности приложения;

b) список требований безопасности приложения для снижения рисков безопасности.

Этих данных должно быть достаточно для того, чтобы команда проекта могла выбрать подходящие МОБП для удовлетворения требований безопасности, т. е. выбрать целевой уровень доверия приложения.

Рисунок 4 иллюстрирует то, что анализ рисков безопасности приложения является важным шагом на пути определения целевого уровня доверия приложения.

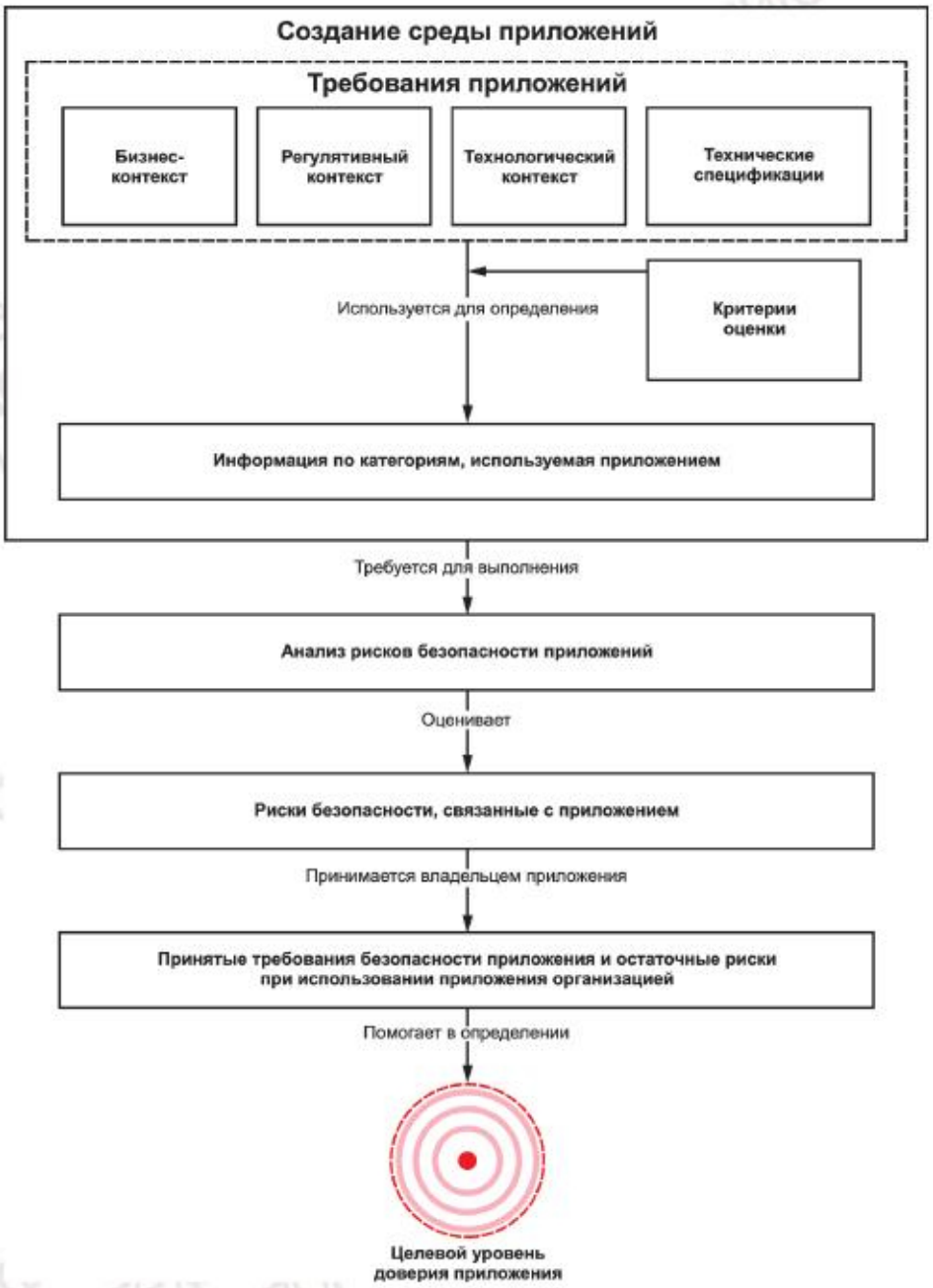

Рисунок 4 — Анализ рисков безопасности приложения как важный шаг на пути определения целевого уровня доверия приложения

Дальнейшие рекомендации по процессу анализа рисков безопасности приложений представлены в ИСО/МЭК 27034-3.

5.5.13 Процесс верификации безопасности приложений

5.5.13.1 Назначение

Назначением данного процесса является определение фактического уровня доверия приложения на любом этапе жизненного цикла приложения.

5.5.13.2 Описание

Это простой процесс, с помощью которого команда верификации анализирует результаты проверочных измерений каждой из МОБП, используемых для достижения целевого уровня доверия приложения.

5.5.13.3 Результаты

Результатами выполнения данного процесса являются:

a) определенный фактический уровень доверия приложения;

b) если фактический уровень доверия приложения равен его целевому уровню доверия приложения, владелец приложения получает документальное подтверждение того, что риски информационной безопасности для этого приложения были снижены до приемлемого уровня.

5.5.13.4 Мероприятия по внедрению

Таблица 17 — Диаграмма RACI для внедрения процесса верификации приложения

Мероприятия по внедрению	Владелец приложения	Группа НСО	Команда верификации	Специалист в предметной области	Аудитор
1) Получение результатов проверочных измерений, проводимых аудитором, для каждой МОБП, используемой для достижения целевого уровня доверия приложения, и подтверждение того, что результат является положительным	A	I	R	C	C

5.5.13.5 Рекомендации

Формальный процесс верификации, определенный политиками верификации, можно выполнять на любом этапе жизненного цикла приложения. Он должен выполняться независимой группой верификации, которая не участвует в проектах по разработке приложений.

В качестве исходных данных необходимо использовать результаты проверочных измерений для каждой МОБП, используемых для достижения целевого уровня доверия приложения.

Проверочные измерения МОБП реализуются с помощью различных методов тестирования, таких как анализ исходного кода и модульное тестирование. На более поздних этапах жизненного цикла можно использовать другие методы верификации, например, тестирование по принципу «белого ящика» или «черного ящика», включая интеграционное тестирование или тестирование на проникновение.

Обзор этого процесса содержится в ИСО/МЭК 27034-1:2011 (рисунок 14). Подробное описание процесса верификации безопасности приложений приведено в ИСО/МЭК 27034-4, где представлены дальнейшие рекомендации по этому процессу.

Приложение А
(справочное)

Согласование НСО и ПМБП с ИСО/МЭК 15288 и ИСО/МЭК 12207 с помощью ИСО/МЭК 15026-4

А.1 Общие положения

ИСО/МЭК 15026-4 («Системная и программная инженерия. Гарантирование систем и программного обеспечения. Часть 4. Гарантия жизненного цикла») предоставляет руководящие принципы и рекомендации по выполнению процессов, мероприятий и задач для анализа определенных свойств систем и программных продуктов, входящих в список особенно важных и требующих проверки свойств, т. е. являющихся критически важными свойствами.

ИСО/МЭК 15026-4 содержит независимый от свойств продукта список процессов, мероприятий и задач, предназначенных для оценки соответствия заявленных свойств и их одобрения. Если заинтересованные стороны выбрали для проверки в качестве важного свойство, связанное с безопасностью приложения, ПМБП предоставляет руководство для подтверждения этих требований.

А.2 Сопоставление

В таблице А.1 приведено сопоставление подразделов ИСО/МЭК 15026-4, ИСО/МЭК 15288 и ИСО/МЭК 12207, элемента ПМБП по ИСО/МЭК 27034-1 и роли элемента ПМБП в критически важных процессах ИСО/МЭК 15026 (все части), чтобы выполнить требования безопасности приложения.

Примечания

1 Хотя все процессы из ИСО/МЭК 15288 и ИСО/МЭК 12207 помогают в разработке, но именно процессы, считающиеся критическими в ИСО/МЭК 15026 (все части), являются наиболее актуальными для НСО и процессов менеджмента НСО. Как и в случае критериев соответствия из ИСО/МЭК 15026 (все части), процессы, связанные с соглашением, проектированием, техническим контекстом и программным обеспечением из ИСО/МЭК 15026 следует задействовать, хотя они не являются целью этого сопоставления.

2 ИСО/МЭК 27034-3 содержит процессы обеспечения безопасности приложений, а также информацию об их взаимоотношениях и согласованности с управленческими и техническими процессами из ИСО/МЭК 15288 и ИСО/МЭК 12207.

3 ИСО/МЭК 27034-4 содержит процессы валидации безопасности приложения, с помощью которых измеряется уровень доверия приложения.

Таблица А.1 — Сопоставление подразделов ИСО/МЭК 15026-4, ИСО/МЭК 15288, ИСО/МЭК 12207 и ИСО/МЭК 27034

Подраздел ИСО/МЭК 15026-4	Пункты ИСО/МЭК 15288 и ИСО/МЭК 12207	Элемент процесса ПМБП (по ИСО/МЭК 27034-1)	Роль элемента ПМБП в критических процессах ИСО/МЭК 15026 (все части)
7.2 Процесс приобретения	ИСО/МЭК 15288:2008 (пункт 6.1.1); ИСО/МЭК 12207:2008 (пункт 6.1.1)	7.3.5 Подготовка к работе и эксплуатация приложения	Если для приложения или программного средства используется приобретаемый ПМБП, то необходимо обеспечить, чтобы в соглашении учитывались методы работы/ожидания в сфере безопасности приложения приобретателя в течение всего жизненного цикла приобретаемого элемента приложения. При планировании обеспечения и эксплуатации приложения необходимо, чтобы приобретаемый элемент приложения вписывался в процессы безопасности приобретающей стороны (или ожидаемые процессы), включая критерии приемки, механизмы доставки, возможность взлома во время доставки, обнаружение аномалий и подделок в элементах приложения по прибытии, условия устранения дефектов, управление обновлениями и т. д.

Продолжение таблицы А.1

Подраздел ИСО/МЭК 15026-4	Пункты ИСО/МЭК 15288 и ИСО/МЭК 12207	Элемент процесса ПМБП (по ИСО/МЭК 27034-1)	Роль элемента ПМБП в критических процессах ИСО/МЭК 15026 (все части)
7.3 Процесс поставки	ИСО/МЭК 15288:2008 (пункт 6.1.2); ИСО/МЭК 12207:2008 (пункт 6.1.2)	7.3.5 Подготовка к работе и эксплуатация приложения	Если ПМБП создавался для приложения или программного средства, которое будет использовать приобретающая сторона, то ПМБП должен внедряться таким образом, чтобы приобретающая сторона получал от поставщика продукт или услугу, соответствующие согласованным требованиям. При планировании обеспечения и эксплуатации приложения необходимо оценить процессы обеспечения безопасности приобретаемого элемента приложения, чтобы они вписывались в процессы безопасности покупателя, включая критерии приемки, механизмы доставки, возможность взлома во время доставки, обнаружение аномалий, обнаружение подделок в элементах приложения по прибытии, условия устранения дефектов, управление обновлениями и т. д.
7.4 Процесс планирования проекта	ИСО/МЭК 15288:2008 (пункт 6.3.1); ИСО/МЭК 12207:2008 (пункт 6.3.1)	7.3.4 Создание и поддержка нормативной структуры приложения	Процессы планирования проекта должны использовать ПМБП и созданные в результате НСП для определения и поддержки модели жизненного цикла, состоящей из этапов, используя определенные модели жизненного цикла безопасности приложения организации. При внедрении процесса менеджмента моделями жизненного цикла необходимо использовать ПМБП для создания стандартных моделей жизненного цикла безопасности приложений организации. В процессе планирования проекта необходимо адаптировать эти организационные процессы к конкретным потребностям проекта
7.5 Процесс менеджмента решений	ИСО/МЭК 15288:2008 (пункт 6.3.3); ИСО/МЭК 12207:2008 (пункт 6.3.3)	7.3.5 Подготовка к работе и эксплуатация приложения	Мероприятия, входящие в процесс принятия решений, должны обеспечить учет последствий использования системы безопасности приложения при принятии решений во время обеспечения и эксплуатации приложения
7.6 Процесс менеджмента рисков	ИСО/МЭК 15288:2008 (пункт 6.3.4); ИСО/МЭК 12207:2008 (пункт 6.3.4)	7.3.5 Подготовка к работе и эксплуатация приложения	Риски, связанные с безопасностью проекта приложений, необходимо в полной мере учитывать в процессе менеджмента рисков при установлении приоритетов, принятии решений, создании и поддержании профиля рисков и обработки рисков. Обеспечение и эксплуатация приложения, а также связанные с этим риски необходимо реалистично оценить, включая риск того, что необходимо будет переделать часть приложения. Необходимо оценить потенциальную возможность недостижения необходимого в рамках проекта уровня безопасности приложения, что может привести к рискам, связанным с сертификацией либо аккредитацией системы, или к невозможности использования программного средства по назначению

Продолжение таблицы А.1

Подраздел ИСО/МЭК 15026-4	Пункты ИСО/МЭК 15288 и ИСО/МЭК 12207	Элемент процесса ПМБП (по ИСО/МЭК 27034-1)	Роль элемента ПМБП в критических процессах ИСО/МЭК 15026 (все части)
7.7 Процесс менеджмента конфигурации	ИСО/МЭК 15288:2008 (пункт 6.3.5); ИСО/МЭК 12207:2008 (пункт 6.3.5)	7.3.5 Подготовка к работе и эксплуатация приложения	Процесс менеджмента конфигурации предназначен для обеспечения и поддержки целостности всех идентифицированных артефактов проекта или процессов. Кроме того, он позволяет заинтересованным сторонам получить к ним доступ. Как обеспечение, так и эксплуатация должны отвечать двум условиям для поддержания приемлемого уровня безопасности приложения: (1) эффективное управление конфигурацией элементов приложения для обеспечения безопасности приложения и (2) обеспечение управления конфигурацией данными об эффективности самой системы безопасности приложения. Примечание — Дополнительные рекомендации по работе с данными методами управления конфигурацией доступны в стандартах ИСО/МЭК 27002 «Информационные технологии. Методы и средства информационной безопасности. Свод норм и правил менеджмента информационной безопасности» и ИСО 10007:2003 «Системы менеджмента качества. Руководящие указания по управлению конфигурацией»
7.8 Процесс менеджмента информации	ИСО/МЭК 15288:2008 (пункт 6.3.6); ИСО/МЭК 12207:2008 (пункт 6.3.6)	7.3.5 Подготовка к работе и эксплуатация приложения	Процесс менеджмента информации необходим для обеспечения безопасности приложений, так как он предоставляет информацию об эффективности системы безопасности приложений заинтересованным сторонам и доставляет массивы данных, показывающие эффективность системы безопасности приложений заинтересованным сторонам, включая регулирующие органы или службы согласования
7.9 Процесс определения требований заинтересованной стороны	ИСО/МЭК 15288:2008 (пункт 6.4.1); ИСО/МЭК 12207:2008 (пункт 6.4.1)	7.3.2 Определение требований и среды приложений	Процесс определения требований заинтересованных сторон предназначен для определения требований к системе, которая будет использоваться для предоставления в определенной среде необходимых услуг пользователям и другим заинтересованным сторонам. В его ходе требования анализируются и на их базе создается общий список требований заинтересованных сторон. В отдельную подгруппу этих требований можно выделить целевой уровень доверия приложения и задокументированные свойства системы безопасности приложений, для эффективной работы которой требуется высокий уровень доверия приложения

Продолжение таблицы А.1

Подраздел ИСО/МЭК 15026-4	Пункты ИСО/МЭК 15288 и ИСО/МЭК 12207	Элемент процесса ПМБП (по ИСО/МЭК 27034-1)	Роль элемента ПМБП в критических процессах ИСО/МЭК 15026 (все части)
7.10 Процесс анализа требований	ИСО/МЭК 15288:2008 (пункт 6.4.2); ИСО/МЭК 12207:2008 (пункт 6.4.2)	7.3.3 Оценка рисков безопасности приложений	Процесс анализа требований предназначен для того, чтобы преобразовать запросы заинтересованных сторон к желаемой услуге в техническое описание требуемого продукта, который мог бы предоставлять эти услуги с целевым уровнем доверия приложения. Анализ требований должен включать в себя оценку рисков безопасности приложений и соответствия требований безопасности приложений, связанных с функциональными границами системы, набором функций, которые должна выполнять система, ограничениями реализации, определенными требованиями заинтересованных сторон или являющимися неизбежными, методами измерения эффективности технического решения (список может быть расширен)
7.11 Процесс верификации	ИСО/МЭК 15288:2008 (пункт 6.4.6)	7.3.6 Проведение аудита безопасности приложения	В контексте ПМБП процесс верификации необходим для подтверждения того, что достигнут целевой уровень доверия приложения. В результате верификации должна быть получена информация, с помощью которой можно было бы выполнить корректирующие действия, позволяющие исправить несоответствия в реализованном приложении или процессах, а также учесть неточности верификации, включая надежность инструментальных средств тестирования и уровень неопределенности результатов (то есть количество ложноположительных и ложноотрицательных срабатываний). В ПМБП должны рассматриваться подтверждающие доказательства, получаемые в ходе жизненного цикла. Например, анализ уязвимостей в процессе разработки или поддержки
7.12 Процесс эксплуатации	ИСО/МЭК 15288:2008 (пункт 6.4.9); ИСО/МЭК 12207:2008 (пункт 6.4.9)	7.3.5 Подготовка к работе и эксплуатация приложения	Процесс эксплуатации включает обеспечение и эксплуатацию приложения с целью предоставления услуг в определенной среде и обеспечения поддержки пользователей программного продукта. При планировании этого процесса необходимо стремиться к поддержанию заданного уровня безопасности приложений на протяжении всего жизненного цикла системы, учитывать эксплуатационные ограничения и согласованность допущений в методе обеспечения безопасности приложений. Необходимо создать системы и процедуры отчетности для проекта, чтобы анализировать и устранять инциденты, связанные с безопасностью приложений

Окончание таблицы А.1

Подраздел ИСО/МЭК 15026-4	Пункты ИСО/МЭК 15288 и ИСО/МЭК 12207	Элемент процесса ПМБП (по ИСО/МЭК 27034-1)	Роль элемента ПМБП в критических процессах ИСО/МЭК 15026 (все части)
7.13 Процесс сопровождения	ИСО/МЭК 15288:2008 (пункт 6.4.10); ИСО/МЭК 12207:2008 (пункт 6.4.10)	7.3.5 Подготовка к работе и эксплуатация приложения	При планировании обслуживания во время обеспечения и эксплуатации приложения необходимо учитывать безопасность приложения на протяжении всего жизненного цикла системы. План сопровождения проекта должен включать оценку влияния на безопасность приложения изменений, внесенных в приложение или элементы системы во время сопровождения, а также постоянно предоставлять доказательства того, что поддерживается целевой уровень доверия приложения

Приложение В
(справочное)

Пример реализации НСО: внедрение ИСО/МЭК 27034 «Безопасность приложений» и НСО в существующей организации

В.1 Общие положения

В этом примере показано, как финансовое учреждение запускает проект по внедрению ИСО/МЭК 27034 «Безопасности приложений» и создает НСО с целью повышения уровня безопасности своих приложений и управления мерами обеспечения безопасности приложений во всех проектах разработки приложений.

Организация решила внедрить ИСО/МЭК 27034, используя пошаговую методику, реализуя проект этап за этапом, в ходе каждого из которых выполняются определенные задачи. В этом примере демонстрируется только первый этап проекта.

Организация разделила проект на шесть подпроектов, как показано на рисунке В.1.

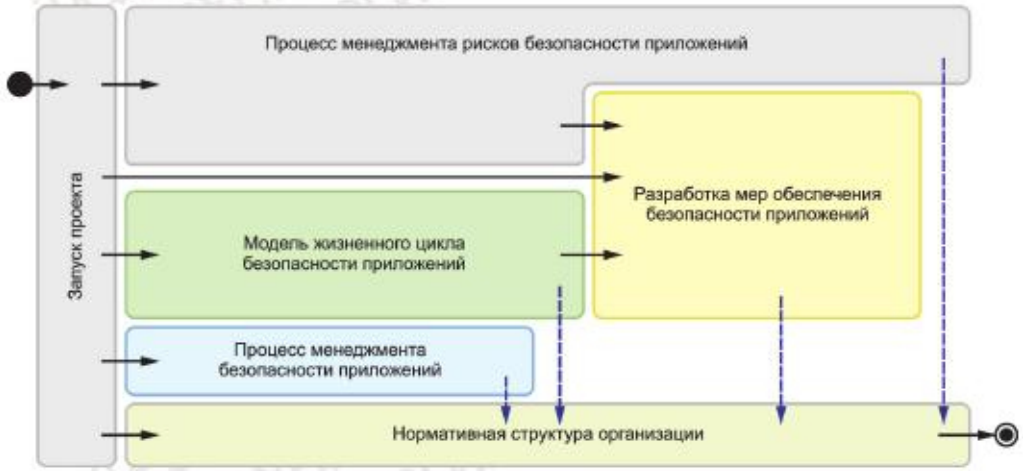

Рисунок В.1 — Внедрение НСО в организации — обзор подпроектов

В.1.1 Запуск проекта

В.1.1.1 Назначение

Назначение этого подпроекта заключается в том, чтобы:

a) определить приемлемый и управляемый объем проекта и каждого подпроекта;
b) назначить проектные команды;
c) определить структуру разрабатываемых МОБП;
d) осуществлять мониторинг подпроектов.

В.1.1.2 Общая информация о подпроекте

Графическое представление подпроекта приведено на рисунке В.2.

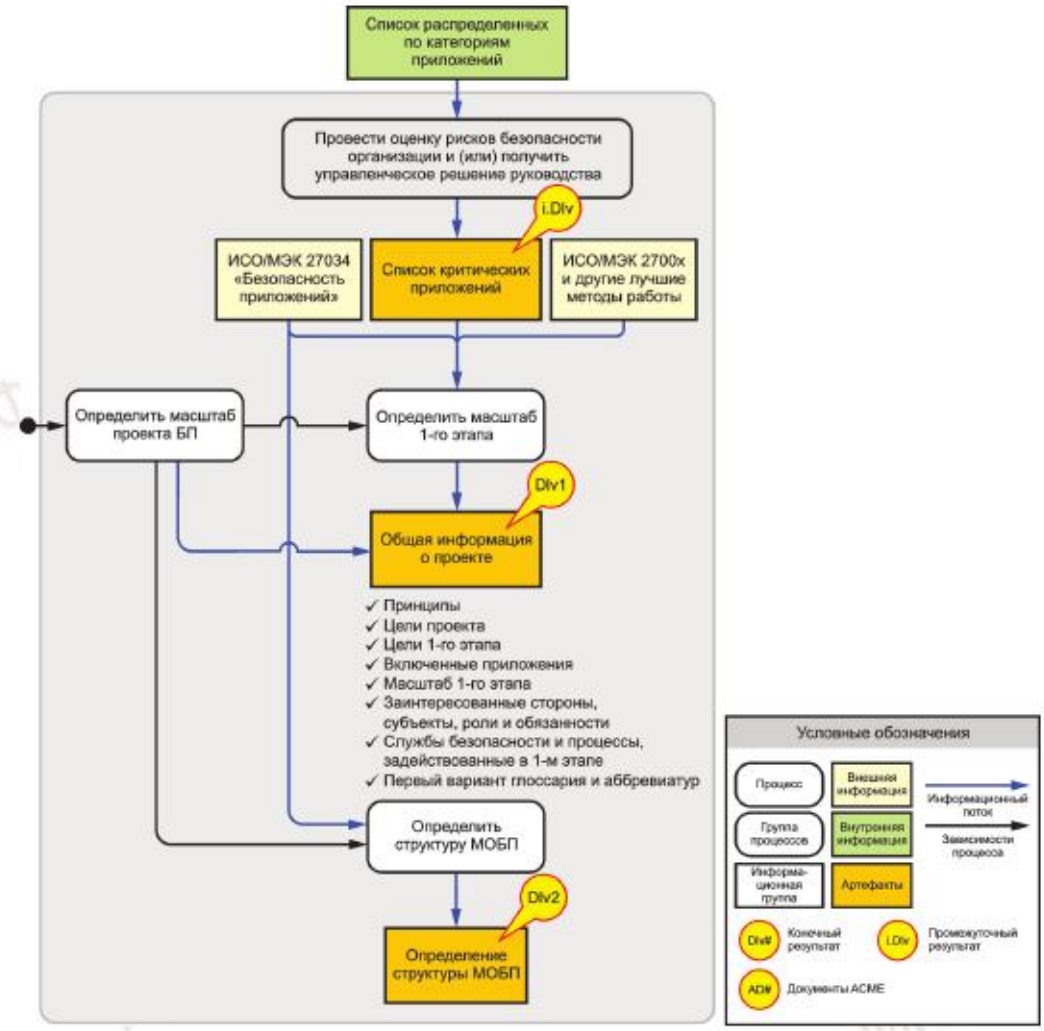

Рисунок В.2 — Проект внедрения НСО для обеспечения безопасности приложений, первый этап

В.1.1.3 Действующие субъекты

К действующим субъектам, участвующим в этом подпроекте, относятся:

a) высшее руководство;

b) менеджер проектов.

В.1.1.4 Исходные данные

Исходными данными для этого подпроекта является список существующих приложений, распределенных по категориям (согласно системе менеджмента информационной безопасности).

В.1.1.5 Мероприятия

Как показано на рисунке В.2, к мероприятиям этого подпроекта относятся:

a) определение масштаба проекта безопасности приложения;

b) проведение оценки рисков безопасности организации и (или) получение управленческого решения высшего руководства;

c) определение масштаба первого этапа проекта согласно пункту b);

d) определение структуры МОБП.

B.1.1.6 Результаты

Результатами этого подпроекта являются:

a) iDiv — список критических приложений;

b) Dlv 1 — общая информация о проекте, содержащая:

1) принципы;
2) цели проекта;
3) цели первого этапа;
4) включенные приложения;
5) масштаб первого этапа;
6) заинтересованные стороны, действующие субъекты, роли и обязанности;
7) службы безопасности и процессы, задействованные в первом этапе;
8) первый вариант глоссария и аббревиатур;

c) Dlv 2 — определение структуры МОБП.

B.1.2 Подпроект менеджмента рисков безопасности приложений

B.1.2.1 Назначение

Во время этого подпроекта организация планирует, реализует, обслуживает и поддерживает:

a) разработку процесса менеджмента рисков безопасности приложений, адаптированного к действующим субъектам, контекстам и спецификациям приложений;

b) выявление рисков безопасности, исходящих от использования организацией критически важных приложений;

c) определение требований безопасности, которые должны выполняться с помощью МОБП.

B.1.2.2 Действующие субъекты

Действующим субъектом этого подпроекта является группа по менеджменту рисков информационной безопасности.

B.1.2.3 Общая информация о подпроекте

Графическое представление этого подпроекта приведено на рисунке B.3.

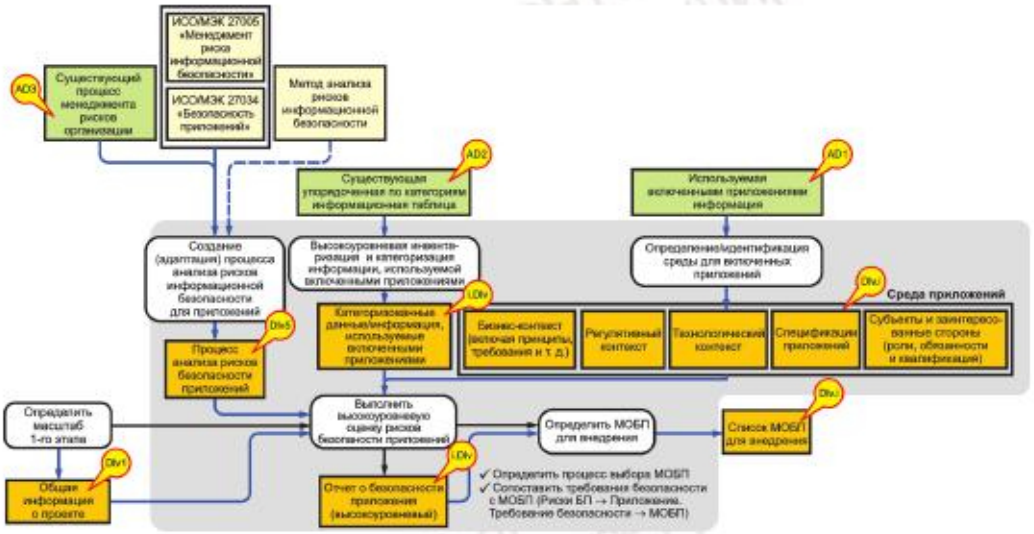

Рисунок B.3 — Подпроект процесса менеджмента рисков безопасности приложений

B.1.2.4 Исходные данные

Исходными данными для этого подпроекта являются:

a) метод анализа рисков информационной безопасности;

b) AD 1 — используемая включенными приложениями информация;

c) AD 2 — существующая упорядоченная по категориям информационная таблица;

d) AD 3 — существующий процесс менеджмента рисков организации;

e) Dlv 1 — общая информация о проекте.

B.1.2.5 Мероприятия

Мероприятия, проводимые в рамках этого подпроекта, заключаются в том, чтобы:

a) создать (адаптировать) процесс анализа рисков информационной безопасности для приложений;

b) провести высокоуровневую инвентаризацию и категоризацию информации, используемой включенными приложениями;

c) определить/идентифицировать среды для включенных приложений;

d) выполнить высокоуровневую оценку рисков безопасности приложений;

e) определить МОБП для внедрения;

1) определить процесс выбора МОБП;

2) сопоставить требования безопасности с МОБП (риски безопасности, требования безопасности МОБП).

B.1.2.6 Результаты

Результатами этого подпроекта являются:

a) Dvl 5 — процесс анализа рисков безопасности приложений;

b) i.Dvl — категоризованные данные/информация, используемые включенными приложениями;

c) i.Dlv — среда приложений;

1) бизнес-контекст (включая принципы, требования и т. д.);

2) регулятивный контекст;

3) технологический контекст;

4) спецификации приложений;

5) действующие субъекты и заинтересованные стороны (роли, обязанности и квалификация);

d) i.Dlv — отчет о безопасности приложения (высокоуровневый);

e) i.Dlv — список МОБП для внедрения.

B.1.3 Подпроект модели жизненного цикла приложения

B.1.3.1 Назначение

Во время этого подпроекта организация планирует, реализует, обслуживает и поддерживает:

a) приведение в соответствие методов, процессов и мероприятий, используемых в разных жизненных циклах в организации;

b) эффективное сотрудничество ответственного руководства и команд, участвующих в управлении, создании архитектуры, верификации на соответствие, разработке, эксплуатации, управлении ИТ, верификации и аудите;

c) определение этапов жизненного цикла в рамках первого этапа.

B.1.3.2 Действующие субъекты

Действующие субъекты, участвующие в этом подпроекте:

a) команда по обеспечению соответствия;

b) команда по разработке ИТ-приложений;

c) команда по управлению проектами;

d) команда по интеграции систем безопасности в проекты;

e) команда по разработке архитектуры безопасности.

B.1.3.3 Общая информация о подпроекте

Графическое представление этого подпроекта приведено на рисунке B.4.

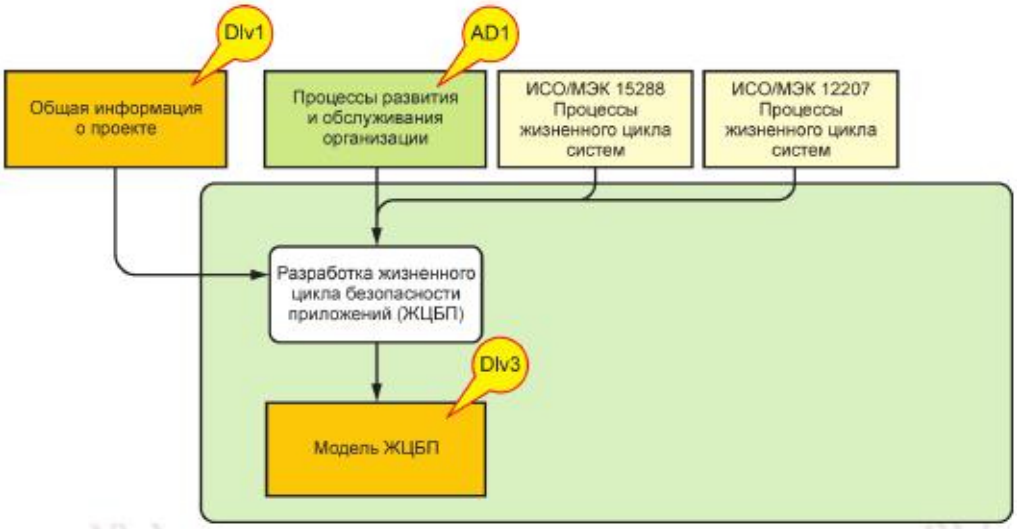

Рисунок В.4 — Подпроект модели жизненного цикла безопасности приложений

В.1.3.4 Исходные данные

Исходными данными для этого подпроекта являются:

a) AD 1 — процессы разработки и обслуживания организации;

b) Dlv 1 — общая информация о проекте.

В.1.3.5 Мероприятия

К мероприятиям этого подпроекта относится разработка жизненного цикла безопасности приложений (ЖЦБП) для организации.

В.1.3.6 Результаты

Результатом этого подпроекта является: Dlv 3 — модель ЖЦБП.

В.1.4 Подпроект процесса менеджмента безопасности приложений

В.1.4.1 Назначение

В ходе этого подпроекта организация планирует, реализует и поддерживает разработку и обслуживание процесса менеджмента безопасности приложений, адаптированного под организацию и соответствующего требованиям ИСО/МЭК 27034.

В.1.4.2 Действующие субъекты

К действующим субъектам, участвующим в этом подпроекте, относятся:

a) команда разработчиков программных средств;

b) команда по управлению проектами;

c) команда по интеграции систем безопасности в проекты.

В.1.4.3 Общая информация о подпроекте

Графическое представление этого подпроекта приведено на рисунке В.5.

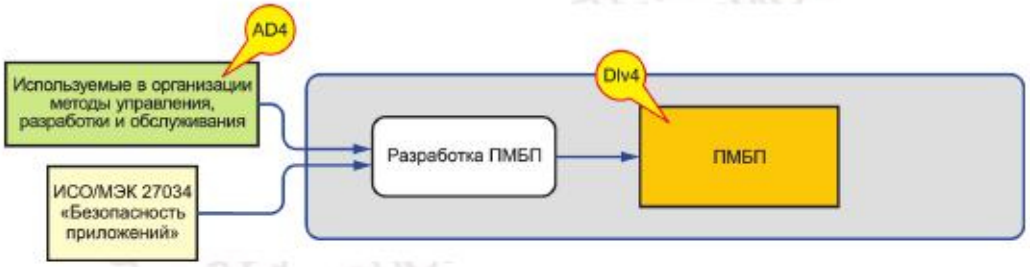

Рисунок В.5 — Подпроект процесса менеджмента безопасности приложений

B.1.4.4 Исходные данные

Исходными данными для этого подпроекта: AD 4 являются используемые в организации методы управления, разработки и обслуживания

B.1.4.5 Мероприятия

К мероприятиям этого подпроекта относится разработка процесса менеджмента безопасности приложений организации.

B.1.4.6 Результаты

Результатом этого подпроекта является: Dlv 4 — ПМБП (документация и руководство по интеграции системы безопасности приложений в проект).

B.1.5 Подпроект нормативной структуры организации

B.1.5.1 Назначение

Во время этого подпроекта организация планирует, реализует, обслуживает и поддерживает:

a) назначение членов группы НСО;

b) разработку процессов управления и обслуживания НСО;

c) консолидацию элементов безопасности приложений в надежном репозитории, доступном всем заинтересованным сторонам.

B.1.5.2 Действующие субъекты

К действующим субъектам, участвующим в этом подпроекте, относятся:

a) команда по обеспечению соответствия;

b) команда по разработке ИТ-приложений;

c) команда по управлению проектами;

d) команда по эксплуатации и поддержке ИТ-инфраструктуры;

e) управление — команда поддержки управления проектами.

B.1.5.3 Общая информация о подпроекте

Графическое представление этого подпроекта приведено на рисунке B.6.

Рисунок B.6 — Подпроект нормативной структуры организации

B.1.5.4 Исходные данные

Исходными данными для подпроекта является текущая архитектура организации.

B.1.5.5 Мероприятия

К мероприятию этого подпроекта относится начало работы группы НСО.

B.1.5.6 Результаты

Результатом этого подпроекта является: i.Dlv — создание нормативной структуры для обеспечения безопасности приложений.

B.1.6 Подпроект разработки мер обеспечения безопасности приложений

B.1.6.1 Назначение

Во время этого подпроекта организация планирует, реализует, обслуживает, поддерживает и проводит аудит:

a) разработка МОБП в соответствии с требованиями безопасности приложений организации;

b) валидация, верификация, тестирование, внедрение и аудит разработанных МОБП;

c) согласование МОБП с моделью жизненного цикла безопасности приложения;

d) управление процессом разработки и поддержки МОБП;

e) разработка обучающих курсов для тех, кто будет разрабатывать и проводить валидацию МОБП;

f) разработка обучающих курсов для тех, кто будет внедрять, проверять и проводить аудит МОБП.

B.1.6.2 Действующие субъекты

К действующим субъектам, участвующим в этом подпроекте, относятся:

a) владельцы включенных приложений;

b) команда по обеспечению соответствия — команда по разработке структуры управления информационной безопасностью;

c) команда разработчиков программных средств;
d) команда по разработке ИТ-приложений.

B.1.6.3 Общая информация о подпроекте

Графическое представление этого подпроекта приведено на рисунке B.7.

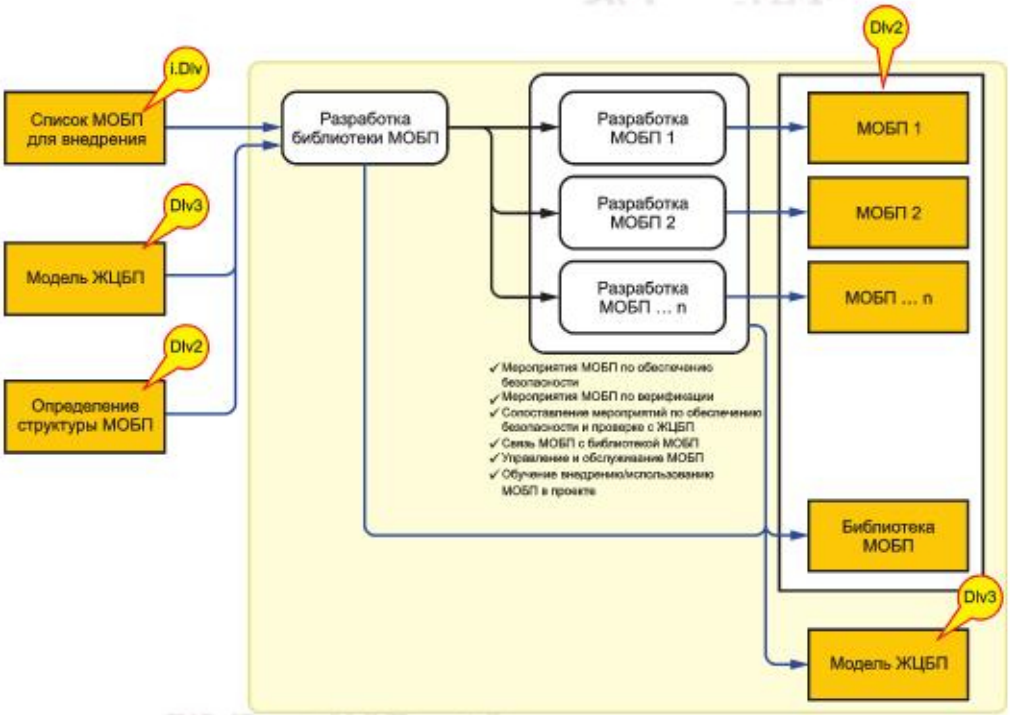

Рисунок B.7 — Подпроект «Разработка мер обеспечения безопасности приложений»

B.1.6.4 Исходные данные

Исходными данными этого подпроекта являются:

a) i.Dlv — список МОБП для внедрения;
b) Dlv 2 — определение структуры МОБП;
c) Dlv 3 — модель ЖЦБП.

B.1.6.5 Мероприятия

Мероприятия для этого подпроекта состоят в следующем:

a) разработать библиотеку МОБП;
b) разработать МОБП с 1, 2 по «n»:
   1) разработать мероприятия по обеспечению безопасности МОБП;
   2) разработать мероприятия по верификации МОБП;
   3) сопоставить мероприятия по обеспечению безопасности и проверке с моделью ЖЦБП;
   4) связать МОБП с библиотекой МОБП;
   5) разработать процесс управления и обслуживания МОБП;
   6) разработать руководство или программу обучения по внедрению/использованию данной МОБП в проекте.

B.1.6.6 Результаты

Результатами этого подпроекта являются:

a) МОБП;
b) библиотека МОБП;
c) Dlv 3 — модель ЖЦБП (обновленная).

B.2 Полная схема рабочего процесса проекта

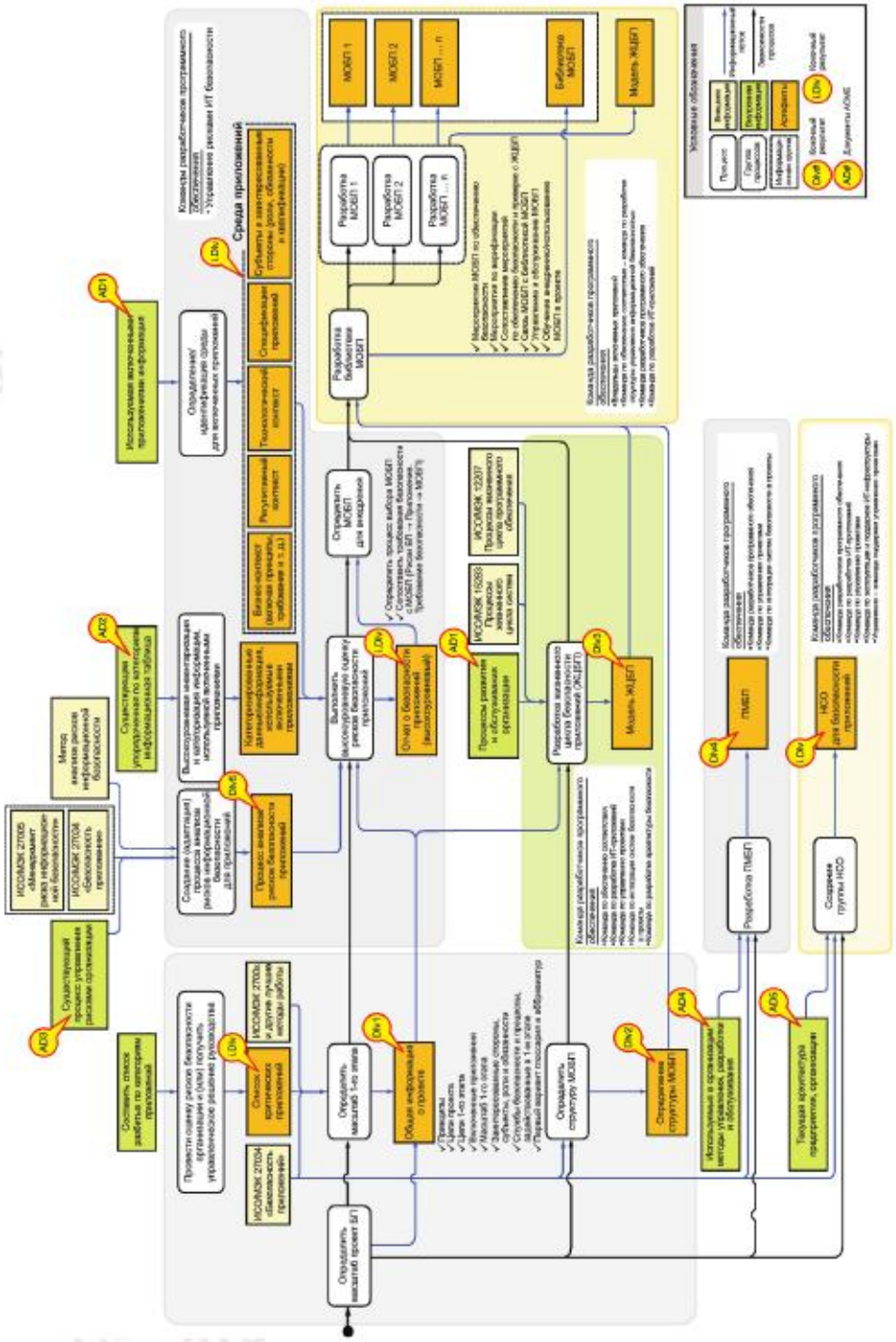

Рисунок В.8 — Пример реализации НСО: внедрение системы безопасности приложений по ИСО/МЭК 27034 и НСО в организации (обзорная диаграмма)

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ISO/IEC 27000	IDT	ГОСТ Р ИСО/МЭК 27000—2021 «Информационные технологии. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»
ISO/IEC 27005	IDT	ГОСТ Р ИСО/МЭК 27005—2010 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности»
ISO/IEC 27034-1:2011	IDT	ГОСТ Р ИСО/МЭК 27034-1—2014 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия»
Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандарта: - IDT — идентичный стандарт.		

Библиография

[1] ISO/IEC 33001:2015, Information technology — Process assessment — Part 1: Concepts and terminology

[2] ISO/DIS 19011:2011, Information technology — Security techniques — Guidelines for auditing management systems

[3] ISO/IEC/TR 20000-4:2010, Information technology — Service management — Part 4: Process reference model

[4] ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements

[5] ISO/IEC 27003:2010, Information technology — Security techniques — Information security management system implementation guidance

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

УДК 006.34:004.056:004.056.5:004.056.53:006.354 ОКС 35.030

Ключевые слова: нормативная структура организации (НСО), нормативная структура приложения (НСП), жизненный цикл безопасности приложений (ЖЦБП), эталонная модель жизненного цикла безопасности приложений (ЭМЖЦБП), процесс менеджмента безопасности приложений (ПМБП), мера обеспечения безопасности приложений (МОБП)

Технический редактор *И.Е. Черепкова*
Корректор *С.В. Смирнова*
Компьютерная верстка *Е.А. Кондрашовой*

Сдано в набор 17.05.2021. Подписано в печать 02.06.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 6,05. Уч.-изд. л. 5,47.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

Создано в единичном исполнении во ФГУП «СТАНДАРТИНФОРМ»
для комплектования Федерального информационного фонда стандартов,
117418 Москва, Нахимовский пр-т, д. 31, к. 2.
www.gostinfo.ru info@gostinfo.ru