ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27034-3— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность приложений

Часть 3

Процесс менеджмента безопасности приложений

(ISO/IEC 27034-3:2018, Information technology — Application security — Part 3: Application security management process, 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. № 351-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27034-3:2018 «Информационные технологии. Безопасность приложений. Часть 3. Процесс менеджмента безопасности приложений» (ISO/IEC 27034-3:2018 «Information technology — Application security — Part 3: Application security management process», IDT).

ИСО/МЭК 27034-3:2018 подготовлен подкомитетом 27 «Методы и средства обеспечения безопасности» Совместного технического комитета ИСО/МЭК СТК 1 «Информационные технологии».

Наименование настоящего стандарта изменено относительно наименования указанного международного стандарта для приведения в соответствие с ГОСТ Р 1.5—2012 (пункт 3.5).

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

0.1 Общие положения

Системный подход к интеграции мер обеспечения безопасности на протяжении всего жизненного цикла приложений способствует обеспечению в организации надежной защиты информации, которая используется и хранится в приложениях.

ИСО/МЭК 27034, состоящий из нескольких частей, предоставляет описание структур и процессов для оказания помощи организациям в планомерной интеграции мер обеспечения безопасности на протяжении жизненного цикла приложений.

Настоящий стандарт содержит описание процессов, необходимых для менеджмента безопасности приложений, которые идентифицируются организацией как критическая информация.

Таблица 1 — Обзор структуры ИСО/МЭК 27034

Область применения	Структура ИСО/МЭК 27034	Описание
Организация	Нормативная структура организации (НСО)	Единый централизованный репозиторий информации о безопасности приложений
	Процесс менеджмента НСО	Процесс сопровождения и постоянного улучшения НСО
Приложение	Нормативная структура приложения (НСП)	Репозиторий для всех мер обеспечения безопасности приложения
	Процесс менеджмента безопасности приложения	Процесс, основанный на оценке риска, который использует НСП для создания и валидации приложений

Как показано в таблице 1, структура и процессы на уровне организации основаны на нормативной структуре организации (НСО). НСО, ее элементы и поддерживающие процессы определены в ИСО/МЭК 27034-2.

Описание структуры и процессов на уровне приложений приведено в разделах 5, 6 и 7 настоящего стандарта. Процесс менеджмента безопасности приложений (ПМБП) помогает проектной группе применять соответствующие части НСО к конкретному проекту приложения и официально регистрировать свидетельства результатов в нормативной структуре приложения (НСП).

Описание процессов определения требований приложения и его среды содержится в 6.1—6.5. Идентификация требований приложения и его среды, а также оценка рисков с точки зрения безопасности приложения описывается в 6.1. Оценка целевого уровня доверия приложения рассматривается в 6.2; создание и поддержание нормативной структуры приложения (НСП), а также меры обеспечения безопасности приложения (МОБП) определены в 6.3; процессы, относящиеся к реализации и эксплуатации приложения, приведены в 6.4. Наконец, в 6.5 содержится описание процесса проверки правильности реализации НСП и МОБП.

0.2 Назначение

Целью настоящего стандарта является определение требований и рекомендаций для процесса менеджмента безопасности приложения и нормативной структуры приложения[1)].

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

0.3 Целевая аудитория

0.3.1 Общие положения

Настоящий стандарт предоставляет лучшие практики для широкой аудитории и будет особенно полезен для следующих категорий лиц:

a) руководителей;
b) членов групп подготовки к работе и эксплуатации;
c) приобретающих сторон;
d) поставщиков;
e) аудиторов;
f) пользователей.

0.3.2 Руководители

Руководители — это лица, вовлеченные в процесс управления приложением. К руководителям относятся:

a) менеджеры по информационной безопасности, включая директора по информационной безопасности (Chief Information Security Officer, CISO);
b) руководители проектов;
c) менеджеры по продуктовой линейке;
d) менеджеры по развитию;
e) владельцы приложений;
f) руководители направления, включая руководителя по информационным технологиям, которые контролируют сотрудников.

Руководители обязаны:

a) обеспечивать, чтобы любые связанные с приложениями проекты, инициативы или процессы были основаны на результатах управления рисками;
b) гарантировать наличие надлежащих проверок информационной безопасности, как того требуют применимые политики и процедуры в области информационной безопасности;
c) осуществлять надзор за реализацией безопасного приложения;
d) информировать всех субъектов о проблемах безопасности, обучать их и осуществлять надзор;
e) обеспечивать баланс между затратами на внедрение и поддержанием безопасности приложений, учитывая риски и ценность этого приложения для организации;
f) обеспечивать соответствие стандартам, законам и нормативным актам согласно контексту приложения;
g) обеспечивать документирование политик и процедур безопасности для приложения;
h) курировать все планы, связанные с безопасностью приложения, во всей сети организации;
i) определять какие меры безопасности, а также верификационные измерения должны применяться и тестироваться;
j) утверждать целевой уровень доверия приложения в соответствии с контекстом, характерным для организации;
k) периодически проверять приложения на наличие слабых мест и угроз безопасности и предпринимать корректирующие и предупреждающие действия;
l) проверять аудиторские отчеты с рекомендациями по одобрению или отклонению приложений с точки зрения надлежащего выполнения необходимых мер защиты приложений;
m) гарантировать, что недостатки безопасности устраняются с помощью методов безопасного кодирования;
n) основывать свои решения на уроках, извлеченных из записей базы знаний.

0.3.3 Члены групп подготовки к работе и эксплуатации

Члены групп подготовки к работе и эксплуатации (проектная группа или команда приложения) — это лица, вовлеченные в проектирование, разработку и поддержку приложения на протяжение всего жизненного цикла. К членам групп подготовки к работе и эксплуатации относятся:

a) архитекторы;
b) аналитики;
c) программисты;
d) специалисты по тестированию;
e) ИТ-администраторы, в том числе системные администраторы, администраторы баз данных, сетевые администраторы и администраторы приложений.

В обязанности членов группы входит:

a) определение того, какие меры обеспечения безопасности приложения необходимо применить на каждом этапе жизненного цикла приложения и с какой целью;

b) определение того, какие меры необходимо реализовать в самом приложении;

c) сведение к минимуму влияния вводимых мер на процессы разработки, тестирования и документирования в течение жизненного цикла приложения;

d) обеспечение соответствия мер обеспечения безопасности необходимым требованиям;

e) получение доступа к инструментальным средствам и лучшим практикам с целью оптимизации процессов разработки, тестирования и документирования;

f) проведение экспертной оценки;

g) участие в планировании и разработке стратегии по приобретению программных средств;

h) организация мероприятий по утилизации остаточных элементов после завершения работы (например, управление имуществом/утилизация).

0.3.4 Приобретающие стороны

В эту категорию входят все лица, вовлеченные в приобретение продукта или услуги.

В обязанности приобретающих сторон входит:

a) установление деловых отношений с целью приобретения необходимых товаров и услуг (например, для объявления тендера, проведения оценки и заключения договоров);

b) подготовка запросов предложений, которые включают в себя описание требований к мерам обеспечения безопасности;

c) выбор поставщиков, которые соответствуют необходимым требованиям;

d) проверка доказательства мер обеспечения безопасности, применяемых аутсорсинговыми службами;

e) оценка продуктов, подтверждающая доказательства правильности внедрения мер обеспечения безопасности приложений.

0.3.5 Поставщики

В эту категорию входят все лица, вовлеченные в поставку продукта или услуги.

В обязанности поставщика входит:

a) соблюдение требований безопасности приложений, определенных в запросах предложений;

b) выбор надлежащих мер обеспечения безопасности приложений с учетом цены и требований, описанных в предложениях;

c) предоставление доказательств надлежащей реализации требуемых мер обеспечения безопасности в предлагаемых продуктах и услугах.

0.3.6 Аудиторы

Аудиторы — лица, которые должны:

a) понимать объем и процедуры, связанные с верификационными измерениями в отношении соответствующих мер обеспечения безопасности приложений;

b) обеспечить уверенность в повторяемости результатов аудита;

c) определить список верификационных измерений, которые будут свидетельствовать о том, что приложение достигло целевого уровня доверия приложения;

d) применять стандартизированные процессы аудита, основываясь на использовании свидетельств, поддающихся проверке, в соответствии с ИСО/МЭК 27034 (все части).

0.3.7 Пользователи

Пользователи должны быть уверены в том, что:

a) развертывание или использование приложения является безопасным;

b) приложение последовательно и своевременно принесет надежные результаты;

c) меры обеспечения безопасности приложений и соответствующие им верификационные измерения реализованы и функционируют надлежащим образом.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность приложений

Часть 3

Процесс менеджмента безопасности приложений

Information technology. Security techniques. Application security. Part 3. Application security management process

Дата введения — 2021—11—30

1 Область применения

Настоящий стандарт содержит подробное описание и рекомендации по внедрению процесса менеджмента безопасности приложений.

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 27034-1, 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)

ISO/IEC 27034-2, Information technology — Security techniques — Application security — Part 2: Organization normative framework (Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 2. Нормативная структура организации)

ISO/IEC 27034-5, Information technology — Security techniques — Application security — Part 5: Protocols and application security controls data structure (Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 5. Структуры данных протоколов и мер обеспечения безопасности приложений)

3 Термины и определения

В настоящем стандарте используются термины по ИСО/МЭК 27034-1, ИСО/МЭК 27034-2, ИСО/МЭК 27000, а также следующие термины с соответствующими определениями.

ИСО и МЭК поддерживают терминологические базы данных для использования в стандартизации в следующих адресах:

- платформа ИСО для онлайн-просмотра: доступна по адресу http://www.iso.org/obp;
- Электропедия МЭК (IEC Electropedia): доступна по адресу http://www.electropedia.org/

Издание официальное

3.1 **аудит безопасности приложения** (application security audit): Систематический, независимый и документированный процесс получения аудиторских доказательств при проверке действий в области безопасности приложения и его объективной оценки для определения степени выполнения критериев аудита, требуемых органом контроля безопасности приложений.

3.2 **проверка безопасности приложения** (application security verification): Процесс анализа и проверки результатов деятельности по обеспечению безопасности приложений путем выполнения верификационных измерений.

Примечания

1 Для организации требуемые элементы НСО и меры безопасности соответствуют спецификациям НСО и процессу менеджмента НСО.

2 Для приложения действия по обеспечению безопасности и связанные с ними действия по проверке и измерению могут быть частью МОБП.

3.3 **критическая информация** (critical information): Информация, которая в случае компрометации может привести к неприемлемому риску.

3.4 **эксперт в предметной области** (domain expert): Человек, который является экспертом в определенной области или теме.

3.5 **менеджмент риска** (risk management): Скоординированные действия по руководству и управлению организацией в отношении риска.

[Руководство ИСО 73:2009, статья 2.1]

Примечание — В настоящем стандарте используется термин «процесс» для описания управления рисками в целом. Элементы процесса менеджмента рисков называются «действиями».

4 Сокращения

БП — безопасность приложений (AS);

МОБП — меры обеспечения безопасности приложений (ASC);

НСО — нормативная структура организации (ONF);

НСП — нормативная структура приложений (ANF);

ПМБП — процесс менеджмента безопасности приложений (ASMP);

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

5 Процесс менеджмента безопасности приложений

5.1 Общие положения

Процесс менеджмента безопасности приложений (ПМБП) — это общий процесс управления безопасностью всех приложений, используемых или разрабатываемых организацией.

Группа НСО отвечает за внедрение и поддержку ПМБП с использованием процесса менеджмента НСО [см. ИСО/МЭК 27034-2:2015 (пункт 5.4.3)]. Эта группа также несет ответственность за обеспечение применения ПМБП ко всем проектам приложений в организации.

Владелец приложения несет ответственность за обеспечение наличия ПМБП для проекта приложения (см. таблицу 3).

В рамках каждого проекта приложения руководитель проекта отвечает за реализацию и использование ПМБП в ходе реализации проекта (см. таблицу 3).

Процесс менеджмента безопасности приложения включает в себя пять этапов:

a) определение среды и требований приложения;
b) оценку рисков, связанных с безопасностью приложения;
c) создание и поддержку нормативной структуры приложения;
d) подготовку к работе и эксплуатацию приложения;
e) аудит безопасности приложения.

Первые три этапа ПМБП направлены на определение и подтверждение соответствующих мер обеспечения безопасности приложения (МОБП) для конкретного приложения. Учитывая, что безопасность

на начальном этапе является основополагающим фактором безопасности приложения, оптимальной точкой для определения требований безопасности для проекта в области программного обеспечения является этап начального планирования. Определение требований безопасности на начальном этапе помогает проектным группам определять ключевые этапы и результаты, а также позволяет интегрировать безопасность таким образом, чтобы свести к минимуму любые нарушения планов и графиков.

Заключительные два этапа ПМБП направлены на внедрение и проверку МОБП.

ИСО/МЭК 27034 (все части) предоставляют компоненты, процессы и структуры, помогающие организации приобретать, внедрять и использовать приложения, которым можно доверять; при этом приемлемость затрат на обеспечение безопасности определяет сама организация. В частности, эти компоненты, процессы и структуры обеспечивают наглядное свидетельство того, что приложения достигают и поддерживают целевой уровень доверия приложения.

Как показано на рисунке 1, эти компоненты, процессы и структуры являются частью двух общих процессов:

a) процесса менеджмента нормативной структуры организации (НСО);

b) процесса менеджмента безопасности приложения (ПМБП).

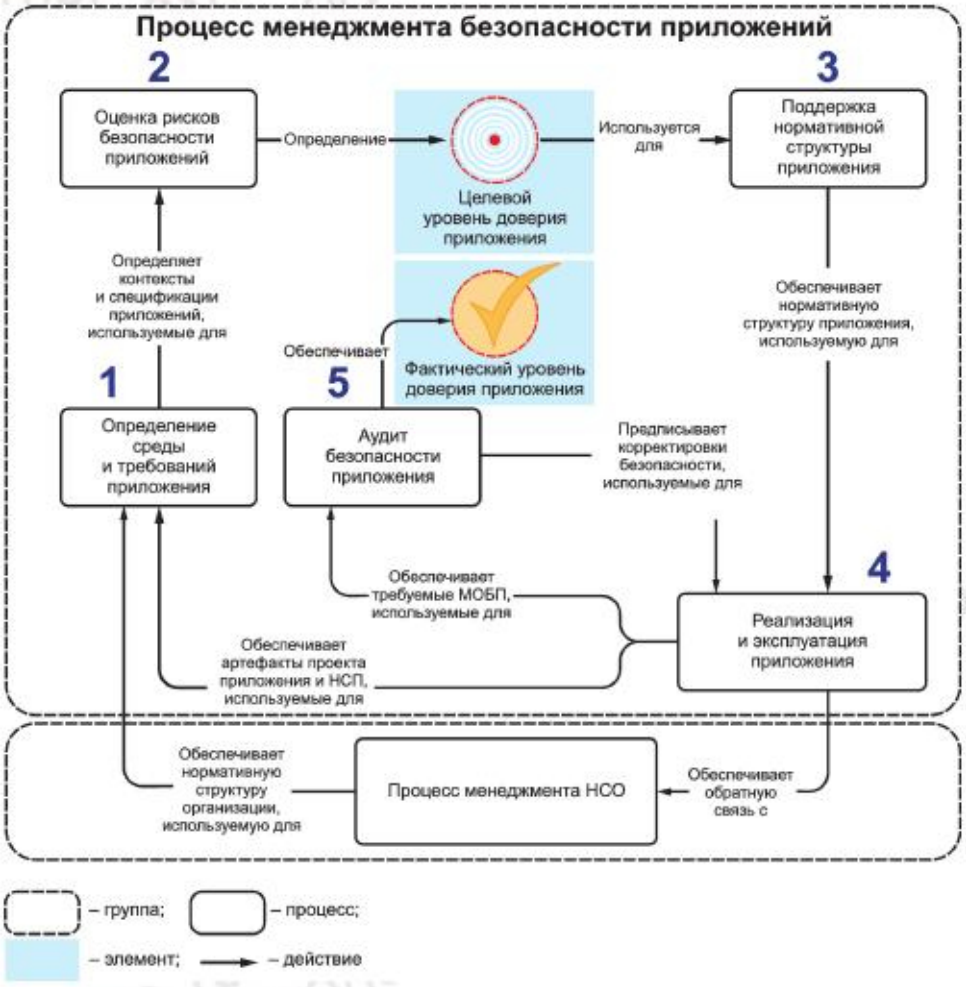

Рисунок 1 — Процесс менеджмента безопасности приложений

Указанные процессы используются в организации на разных уровнях и временных интервалах, а также имеют разные цели. Процесс менеджмента НСО (см. ИСО/МЭК 27034-2) представляет собой непрерывный процесс организационного уровня, а ПМБП используется для управления безопасностью в каждом конкретном проекте приложения.

5.2 Назначение

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

5.3 Принципы и понятия

5.3.1 Общие положения

В дополнение к принципам, определенным в ИСО/МЭК 27034-1, организации, создающие, эксплуатирующие или сопровождающие приложения, должны руководствоваться следующими принципами:

a) каждому приложению должен быть присвоен целевой уровень доверия приложения;

b) любой компонент или процесс в сфере безопасности, используемый в проекте приложения, должен быть выбран из НСО;

c) все выбранные МОБП с целевым уровнем доверия приложения должны быть внедрены, верифицированы и для них должен быть проведен аудит.

5.3.2 Определение 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 субъекты, ответственные, отчитывающиеся, консультирующие и сообщающие о выполнении действий. Для описания обязанностей субъектов используются сокращения (таблица 2).

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

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

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

Очень важно, чтобы организация определила лиц, ответственных, отчитывающихся, консультирующих и сообщающих о выполнении действий по реализации и верификации. Таблица 2 может быть использована при внедрении нормативной структуры приложений в организации.

5.3.3 Взаимосвязь процесса менеджмента безопасности приложений с нормативной структурой организации

НСО, подробно описанная в ИСО/МЭК 27034-2, обеспечивает контекст для ПМБП на уровне организации. Этот контекст включает в себя все процессы, связанные с безопасностью приложений, такие как нормативные акты, законы, лучшие практики, роли и обязанности, принимаемые организацией. ПМБП использует этот контекст для создания и поддержки нормативной структуры приложения для каждого проекта приложения. В свою очередь ПМБП поддерживает постоянное улучшение НСО, основываясь на новых знаниях, предложениях и практиках по совершенствованию мер обеспечения безопасности приложений, полученных в ходе разработки и развертывания приложения.

5.3.4 Использование утвержденных инструментальных средств

Проектные группы должны использовать преимущества новых методов обеспечения безопасности и защиты, используя утвержденные инструментальные средства и связанные с ними проверки

---

1) Ответственный за выполнение действия — Отчитывающийся за выполнение действия — Консультирующий во время выполнения действия — Сообщающий о выполнении действия (RACI).

безопасности, такие как опции компилятора/компоновщика и предупреждения. Список утвержденных инструментальных средств должен быть представлен как часть нормативной структуры организации. Если проектной группе известно об инструментальном средстве, которое превосходит по своим параметрам средства, указанные в утвержденном списке НСО, она должна использовать процесс обратной связи НСО и проинформировать команду НСО об этом инструментальном средстве.

Примечание — Описание, назначение и роль группы НСО определены в ИСО/МЭК 27034-2:2015 (пункт 5.4.3).

5.3.5 Уровень доверия приложения

«Уровень доверия приложения» — это метка, которая присваивается набору применимых МОБП из библиотеки мер обеспечения безопасности приложений в НСО. ИСО/МЭК 27034 (все части) предлагает два типа уровней доверия приложений, которые могут быть связаны с приложением:

a) целевой уровень доверия приложения;

b) фактический уровень доверия приложения.

Целевой уровень доверия приложения должен быть определен в результате реализации процесса менеджмента рисков, приведенного в ИСО/МЭК 27005.

5.3.6 Целевой уровень доверия приложения

Применимые меры обеспечения безопасности для целевого уровня доверия приложения могут быть заранее определены в НСО или получены из рабочего процесса, определяющего эти меры с учетом выбранного уровня доверия приложения и требований безопасности приложения. Для обеспечения согласованности процесса в нескольких приложениях в ходе рабочего процесса могут быть использованы средства автоматизации и инструментальные средства, включая системы управления жизненным циклом приложений.

В процессе оценки рисков устанавливаются требования безопасности, на основании которых определяется целевой уровень доверия приложения. Это, в свою очередь, является целью проектной группы приложения.

Целевой уровень доверия приложения может помочь в достижении уровня доверия приложения, необходимого организации, которая может использовать или развернуть приложение после принятия остаточных рисков, определенных в результате их оценки.

Целевой уровень доверия приложения крайне важен для безопасности приложения, поскольку он напрямую определяет подходящие меры обеспечения безопасности приложения, которые необходимо выбрать из библиотеки МОБП и реализовать в жизненном цикле приложения.

Целевой уровень доверия приложения должен принадлежать одному из уровней доверия приложения (или находится в пределах диапазона), определенных в библиотеке МОБП организации [см. ИСО/МЭК 27034-1:2011 (подпункт 8.1.2.6)], которая является частью НСО.

Библиотека МОБП (ИСО/МЭК 27034-1:2011, рисунок 5) может быть представлена в виде таблицы, в столбце которой находится целевой уровень доверия приложения. Таким образом, выбор уровня доверия приложения означает выбор всех МОБП в этом столбце.

Ниже представлены примеры разбивки уровней доверия приложений, которые могут быть определены организацией.

Примеры

1 Критически важные бизнес-приложения, внутренние приложения, общедоступные приложения.

2 Универсальное общедоступное веб-приложение: целевой уровень доверия приложения — это общедоступное приложение, технологический контекст — веб-приложение с базой данных, бизнес-контекст — приложение хранит и обрабатывает пароли конечных пользователей.

5.3.7 Фактический уровень доверия приложения

Фактический уровень доверия приложения — это максимальный уровень доверия приложения, подтвержденный группой проверки в соответствии с измерениями всех МОБП приложения.

Каждое МОБП, включенное в НСП для любого проекта приложения, предоставляет конкретное и подробное описание действий по измерениям, которые должна выполнить группа проверки, с указанием конкретного этапа жизненного цикла приложения, на котором должно быть выполнено измерение.

Фактический уровень доверия приложения определяется во время проверки безопасности приложения путем проверки МОБП, которая должна быть выполнена в определенный момент жизненного цикла приложения. Если какая-либо МОБП дает сбой в ходе проверки, организация должна принять соответствующие меры для исправления ситуации.

Достижение целевого уровня доверия приложения подтверждается успешной проверкой всех его МОБП и после получения всех необходимых доказательств в результате измерений.

Если некоторые из МОБП не проходят проверку, владелец приложения должен принять необходимые меры для решения этой проблемы.

Учитывая, что целевой уровень доверия приложения был утвержден владельцем приложения на этапе 2 ПМБП, приложение будет считаться безопасным для использования или развертывания в течение определенного периода времени по согласованию с группой проверки, предоставляющей доказательства того, что целевой уровень доверия приложения был достигнут. Статус безопасности приложения действителен только в течение определенного периода времени, поскольку этап 2 ПМБП подлежит периодическому пересмотру.

Приложение считается безопасным в соответствии с ИСО/МЭК 27034, если фактический уровень доверия приложения равен или превышает целевой уровень доверия приложения; например, если все МОБП для уровня доверия приложения «Синий» успешно внедрены и проверены, то приложение может считаться безопасным и получает «Фактический уровень доверия приложения — Синий».

5.3.8 Влияние настоящего стандарта на проект приложения

Типовой проект приложения (до того, как организация учтет рекомендации настоящего стандарта) управляется группой исполнения, применяющей процессы, которые часто автоматизируются с помощью технологий с целью создания прикладного продукта. Роль группы проверки может взять на себя группа обеспечения качества, которая следует планам тестирования для оценки функциональности приложения в соответствии с принятыми функциональными требованиями.

На рисунке 2 показано, как настоящий стандарт помогает добавить новые роли, обязанности, компоненты и процессы в типовой проект приложения.

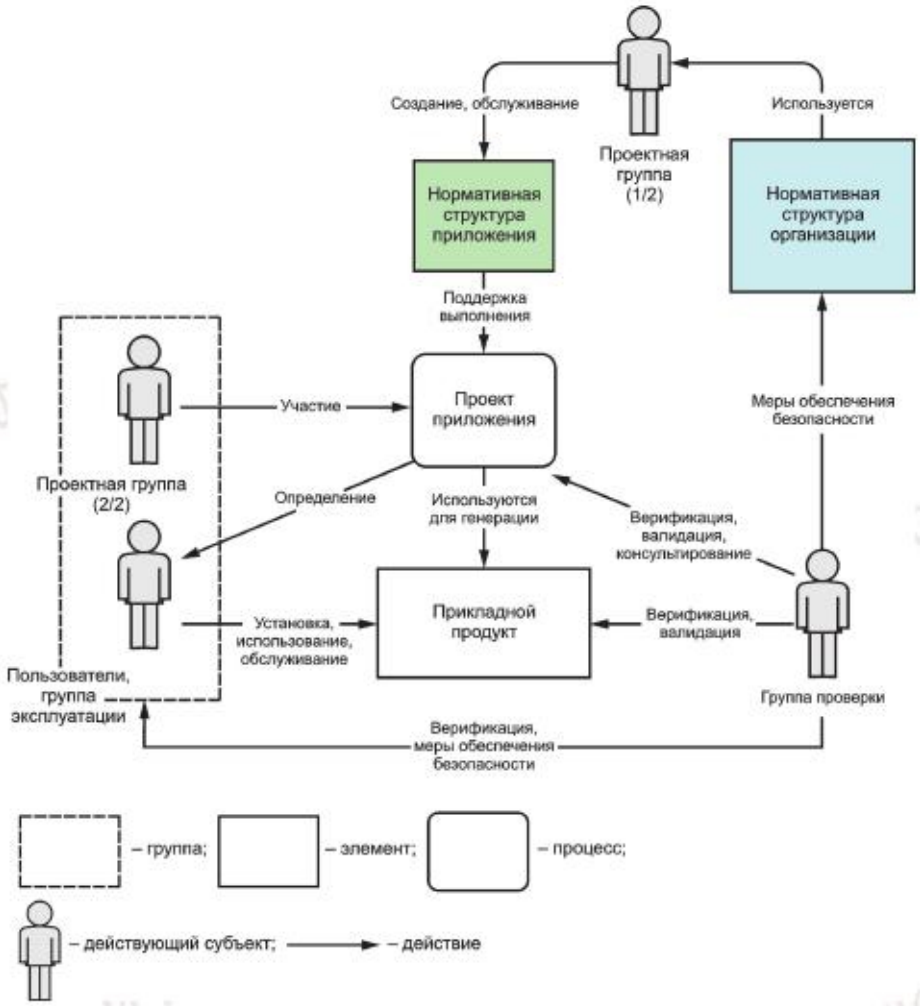

Рисунок 2 — Влияние настоящего стандарта на роли и обязанности в типовом проекте приложения

Технология и методология разработки, используемые группой исполнения, зрелость процесса, качество произведенных артефактов и квалификация участников проекта проверяются редко, и такие проверки, если они выполняются, обычно не формализованы.

6 Этапы процесса менеджмента безопасности приложений

6.1 Определение среды и требований приложения

6.1.1 Общие положения

Идентификация среды приложения позволяет организации определять контексты приложения (бизнес-контекст, технологический контекст, регулятивный контекст), основные характеристики, участников и процессы, а также информацию, связанную с получением и использованием приложения.

Данный этап соответствует шагу «Определение контекста» в процессе менеджмента рисков, приведенном в ИСО/МЭК 27005. В нем представлена необходимая информация для последующих этапов оценки рисков.

Первый этап ПМБП направлен на установление всех требований приложения, в том числе:

a) действующие субъекты;

b) спецификации;

c) информация;

d) среда.

Среда приложения состоит:

a) из технологического контекста;

b) бизнес-контекста;

c) регулятивного контекста.

Подробнее описание контекстов приведено в ИСО/МЭК 27034-1:2011 (подпункты 8.1.2.1—8.1.2.2).

6.1.2 Назначение

Целью данного этапа является сбор необходимой информации в отношении требований безопасности и обеспечение поддержки соответствующих действий ПМБП. Данный этап необходим для того, чтобы:

a) определить владельца приложения;

b) идентифицировать, провести инвентаризацию и консолидировать информацию для анализа рисков безопасности приложений;

c) определить предварительную версию НСП.

6.1.3 Результаты

Основные результаты данного этапа включают в себя:

a) определение лица, официально назначенного владельцем приложения;

b) предварительную нормативную структуру приложения, в том числе:

1) краткое описание трех контекстов;

2) функциональные и нефункциональные требования;

3) архитектуру приложения (в том числе с учетом среды эксплуатации);

4) информационные группы, участвующие в подготовке и эксплуатации приложения.

6.1.4 Мероприятия по реализации

В таблице 3 приведены роли и обязанности, связанные с действиями по реализации процесса «Определение среды и требований приложения».

Таблица 3 — Диаграмма RACI для процесса «Определение среды и требований приложения»

Мероприятия по реализации	Группа НСО	Владелец приложения	Менеджер проекта
1) Определение и назначение владельца приложения	A/R		
2) Реализация ПМБП в проекте		A	R
3) Определение потребностей организации, влияющих на характеристики приложения	A	A/R	I
4) Определение требования приложения, то есть все требования и спецификации, которым должно соответствовать приложение	C	A/R	I
5) Идентификация и классификация информационных групп, используемых приложением, и потока информации между компонентами приложения, а также между приложением и другими системами (см. рисунок 1)	C	A/R	I
6) Определение бизнес-контекста приложения, включая процессы, участников и бизнес-требования, связанные с реализацией и использованием приложения	A/R		
7) Определение регулятивного контекста приложения, т. е. законов и нормативных актов, которые применяются к приложению	C	A/R	I

Окончание таблицы 3

Мероприятия по реализации	Группа НСО	Владелец приложения	Менеджер проекта
8) Определение технологического контекста приложения, т. е. все ИТ-компоненты, необходимые для разработки, развертывания, мониторинга и обслуживания приложения	C	A/R	C/I
9) Валидация, верификация и интегрирование результатов этой деятельности в предварительную НСП	C	A/R	C/I

6.1.5 Мероприятия по верификации

Роли и обязанности, связанные с действиями по верификации процесса «Определение среды и требований приложения», приведены в таблице 4.

Таблица 4 — Диаграмма RACI для верификации процесса «Определение среды и требований приложения»

Мероприятия по верификации	Группа НСО	Менеджер проекта	Владелец приложения	Аудиторы	Проектная группа
1) Подтверждение того, что владелец приложения был назначен для этого проекта приложения	A			R	
2) Сбор документации о контекстах безопасности приложений (бизнес-контекст, регулятивный и технологический контексты)		C	I	A/R	C
3) Сбор спецификации приложения и описание связанных с ним процессов		C	I	A/R	C
4) Сбор классифицированных информационных групп и диаграмм потоков информации.		C	I	A/R	C
5) Сбор доказательств того, что действующие субъекты были идентифицированы, и сведения о каждом из них были задокументированы		C	I	A/R	C
6) Сбор спецификаций приложений, документов с требованиями и архитектурных диаграмм		C	I	A/R	C

6.1.6 Рекомендации

6.1.6.1 Общие положения

Процесс, определяющий требования и среду приложения, включает в себя идентификацию компонентов, начиная с действующих субъектов.

Выявленные действующие субъекты предоставляют информацию для определения среды и контекста приложения.

Действия, необходимые для определения требований и среды приложения, включают в себя:

a) определение действующих субъектов;

b) определение спецификации организационной безопасности приложения;

c) анализ информации, используемой приложением;

d) определение среды приложения.

6.1.6.2 Определение действующих субъектов

При определении действующих субъектов необходимо указать ожидаемые роли, обязанности и квалификации.

После определения действующих субъектов рекомендуется привлечь их к процессу реализации, поскольку они могут предоставить информацию, необходимую для определения среды и контекста приложения.

Компоненты должны быть задокументированы с учетом вариантов, применимых к каждому компоненту в рамках нормативной структуры организации. Кроме того, необходимо сохранить доказательства сбора информации, чтобы на последующих этапах можно было проверить ее правильность.

6.1.6.3 Определение спецификации организационной безопасности приложения

Спецификации безопасности приложения могут быть получены на данном этапе из источников проекта приложения в организации, таких как:

a) спецификации требований к программному обеспечению, например TLS[1], SSH[2], SFTP[3];
b) политики безопасности организации, включая требования к паролю;
c) нормативно-правовые документы;
d) организационные и бизнес-цели и (или) видения;
e) архитектурные диаграммы.

6.1.6.4 Анализ информации, используемой приложением

Потоки информации, относящейся к приложению, должны быть проанализированы и названы, включая данные, предоставленные любым пользователем, потоки данных приложения от интерфейса к серверу, данные, передаваемые приложением, данные, полученные из технологических процедур, структуры данных, данные конфигурации и хранимые данные.

Поток пакетов данных во внутренней сети имеет решающее значение с точки зрения проверки запрашиваемых данных от источника до места назначения.

6.1.6.5 Развертывание среды приложения

Среда приложения определяется путем подробного описания его технологического, регулятивного контекстов и бизнес-контекста.

Примечание — Для создания НСП необходимо задокументировать всю значимую информацию, полученную в результате реализации каждого мероприятия, а также проверить правильность информации и самого процесса на последующих этапах.

Следующие примеры описывают процессы и действия, которые организации могут выполнить на данном этапе.

Примеры

1 Организации могут выполнить первоначальный анализ требований безопасности на начальном этапе проекта, чтобы определить бизнес-контекст, технологический и регулятивный контексты.

2 Организации могут согласовать МОБП для каждого этапа разработки. МОБП содержат заранее определенные процессы обеспечения безопасности и выполнения верификации, критерии и ожидаемые результаты для обработки ошибок или угроз для безопасности приложения. Например, они могут согласовать, что все уязвимости вида SQL[4]-инъекция, должны быть отработаны и исправлены определенным образом до проверки кода.

3 Организации могут классифицировать свои МОБП как «обязательные», «важные» и «желательные» и использовать эту классификацию для определения допустимых пороговых уровней ошибок, чтобы сообщить заинтересованным сторонам пороговые значения серьезности устраненных уязвимостей системы безопасности. Эти пороговые значения можно рассматривать как целевой уровень доверия приложения, который применяется ко всему проекту приложения. Например, организация может определить уровень доверия приложения, требующий, чтобы все «обязательные» и «важные» МОБП для устранения известных «критических» или «высоких» уязвимостей, были реализованы в приложении на момент его выпуска. В этом примере допустимый пороговый уровень ошибки требует, чтобы по крайней мере все «обязательные» и «важные» МОБП были успешно реализованы и верифицированы.

4 Организации могут использовать инструменты для сбора данных о характеристиках и угроз безопасности приложения, чтобы сформировать профиль приложения и, следовательно, список применимых требований безопасности для идентификации соответствующих МОБП. Использование инструментальных средств и средств автоматизации повышают согласованность требований безопасности многих приложений. Инструментальные средства также можно использовать для управления целевыми уровнями доверия приложений и их единообразного применения для различных приложений.

Примечание — Чтобы свести к минимуму негативное воздействие на организации и уменьшить сопротивление со стороны заинтересованных сторон, которые внедряют или используют настоящий стандарт, не требуется от организаций принятия или изменения какого-либо конкретного словаря, имен действующих субъектов

---

[1] *Сетевой протокол транспортного уровня (протокол TCP).*

[2] *Сетевой протокол прикладного уровня (протокол SSH).*

[3] *Сетевой протокол прикладного уровня (протокол SFTP).*

[4] *Язык структурированных запросов (SQL).*

или названий процессов, которые должны быть реализованы. Настоящий стандарт не зависит от методологии разработки и процессов эксплуатации и может быть адаптирован/интегрирован для любого из них.

6.2 Оценка рисков безопасности приложений

6.2.1 Общие положения

Второй этап ПМБП соответствует процессу оценки риска для конкретного проекта приложения.

Данный этап соответствует этапу «Оценка риска информационной безопасности» и части этапа «Обработка рисков информационной безопасности» процесса менеджмента рисков, приведенном в ИСО/МЭК 27005, но с более высоким уровнем детализации и областью действий, ограниченной одним проектом приложения.

Согласно ИСО/МЭК 27005 «в процессе оценки риска устанавливается ценность информационных активов, выявляются потенциальные угрозы и уязвимости, которые существуют или могут существовать, определяются существующие меры безопасности и их воздействие на идентифицированные риски, определяются возможные последствия и, наконец, назначаются приоритеты установленным рискам, а также осуществляется их ранжирование по критериям оценки риска, зафиксированным при установлении контекста».

Процесс оценки рисков включает в себя этапы определения, анализа и оценки рисков. К данному этапу ПМБП также относится «выбор вариантов обработки рисков» для определения приемлемого и утвержденного уровня риска. Поэтому данный этап соответствует этапу «выбор вариантов обработки рисков» в процессе менеджмента рисков, приведенном в ИСО/МЭК 27005.

Данный этап ПМБП также устанавливает требования безопасности приложения, которые будут использованы для выбора необходимых МОБП для приложения, как показано на рисунке 3.

Рисунок 3 — Логический поток от рисков безопасности приложения к снижению рисков

Риски безопасности приложения, вытекающие из его контекста и среды [которые определены на шаге 1 (подраздел 6.1)], устанавливают требования безопасности и соответствующий набор применимых МОБП. На рисунке 3 обозначение «n..n» соответствует отношению «многие ко многим», а «1..n» — «один ко многим».

Этап оценки риска ПМБП завершается определением целевого уровня доверия приложения [см. ИСО/МЭК 27034-1:2011 (пункт 8.2.4)], который должен быть одобрен его владельцем.

Примечания

1 Методология анализа рисков безопасности на уровне организации, возможно, не позволяет идентифицировать все риски и обеспечения безопасности, необходимые для безопасной эксплуатации приложения. Чтобы используемый метод анализа рисков безопасности был эффективен, он должен быть специально разработан или адаптирован; в этом случае данный метод анализа позволит гарантировать, что специфические особенности приложения и его среды принимаются во внимание.

2 Для приложений, которые работают с персональными данными, риски для конфиденциальности также учитываются в процессе оценки риска.

3 Риски для конфиденциальности зависят от применимых законов о неприкосновенности частной жизни и местных нормативных актов, которые упоминаются в регулятивном контексте.

6.2.2 Назначение

Задачей процесса оценки рисков является:

a) для проекта: определить, проанализировать и оценить риски для безопасности, сформулировать итоговые требования безопасности, целевой уровень доверия приложения и необходимые МОБП для защиты приложения;

b) для организации: консолидировать и поддерживать информацию о рисках, связанных с приложением, в НСО.

6.2.3 Результаты

Результатами выполнения мероприятий данного процесса являются:

a) создание предварительной версии НСП, которая содержит информацию о среде приложения, а также информацию, полученную в результате выполнения этого процесса, в том числе:

1) список угроз для безопасности приложения;

2) требования безопасности для снижения рисков;

3) целевой уровень доверия приложения, определяющий список МОБП, которые потребуются в течение жизненного цикла приложения;

b) обновление информации о безопасности приложения в НСО.

6.2.4 Мероприятия по реализации

В таблице 5 показаны роли и обязанности по выполнению действий в ходе реализации процесса «Оценка рисков безопасности приложения».

Таблица 5 — Диаграмма RACI для реализации этапа ПМБП «Оценка рисков безопасности приложения»

Мероприятия по реализации	Группа НСО	Владелец приложения	Проектная группа
1) Выявление и оценка рисков безопасности, связанных с приложением	C	A/R	C
2) Выявление и оценка степени, в которой ранее выявленные угрозы безопасности были устранены в приложении	C	A	R
3) Определение минимальных требований безопасности для приложения (с учетом недопустимых угроз безопасности)	C	A/R	C
4) Определение целевого уровня доверия приложений для приложения, отвечающего всем определенным требованиям безопасности	C	A/R	C
5) Подтверждение и утверждение целевого уровня доверия приложения	I	A	R
6) Сбор информации по результатам анализа рисков в соответствии с 6.1.3	C	A/R	C
7) Обновление содержимого НСП	A	I	R
8) Обновление содержимого НСО	A/R	C	C
9) Обеспечение доступности к информации заинтересованных сторон	I	A/R	I

6.2.5 Мероприятия по верификации

В таблице 6 приведены роли и обязанности, связанные с действиями по верификации процесса «Определение среды и требований приложения».

Таблица 6 — Диаграмма RACI для верификации этапа ПМБП «Оценка рисков безопасности приложения»

Мероприятия по верификации	Менеджеры	Владелец приложения	Группа проверки
1) Сбор исходных данных и результатов анализа рисков безопасности приложений	C	C/I	A/R
2) Сбор исходных данных и результатов анализа рисков безопасности приложения	C	C/I	A/R
3) Гарантия того, что риск безопасности приложения был точно оценен с учетом определенного набора мер обеспечения безопасности приложения	C	C/I	A/R
4) Подтверждение того, что целевой уровень доверия приложения был определен и утвержден	C	C/I	A/R
5) Подтверждение того, что владелец приложения согласился с остаточными рисками, связанными с приложением	C	C/I	A/R

6.2.6 Рекомендации

6.2.6.1 Область оценки рисков для безопасности приложения

Во время оценки рисков следует учитывать риски, связанные с процессами, действиями и действующими субъектами, участвующими в четырех уровнях жизненного цикла безопасности приложений (см. рисунок 4). Важно отметить, что жизненный цикл включает в себя не только этапы подготовки. Риски, относящиеся к этапам эксплуатации, не менее важны.

Поэтому ПМБП распространяется на все этапы и уровни жизненного цикла. Это особенно актуально для организаций, эксплуатирующих приложения, в отличие от организаций, которые выступают только как поставщики.

Рисунок 4 — Пример жизненного цикла безопасности приложения

6.2.6.2 Идентификация рисков, связанных с приложением

Идентификация рисков для безопасности приложения — это процесс поиска, распознавания и описания рисков, касающихся информации, получаемой, хранимой, обрабатываемой, используемой и передаваемой приложением. Следует учитывать риски, независимо от того, находится ли их источник под контролем организации, включая бизнес-контекст, регулятивный и технологический контексты.

Идентификация рисков включает в себя идентификацию источников риска, событий, их причин и потенциальных последствий. Здесь следует учитывать исторические данные, теоретический анализ, обоснованные и экспертные мнения, потребности заинтересованных сторон.

6.2.6.3 Анализ рисков, связанных с приложением

6.2.6.3.1 Общие положения

Анализ рисков является первым шагом в процессе оценки риска. Анализ рисков для приложений часто выполняется в два этапа:

a) высокоуровневый анализ рисков;

b) детальный анализ рисков.

6.2.6.3.2 Высокоуровневый анализ рисков безопасности приложения

Процесс высокоуровневого анализа рисков безопасности приложения обычно выполняется на этапе подготовки в жизненном цикле приложения, как приведено в ИСО/МЭК 27034-1:2011 (подпункт 8.2.2.1).

Высокоуровневый анализ рисков представляет собой простой эмпирический метод для определения целевого уровня доверия приложения согласно базовым спецификациям, а также регулятивному и технологическому контекстам совместно с бизнес-контекстом.

Владелец конкретного проекта приложения должен четко определить роль с обязанностью проводить этот анализ с помощью адекватной методологии на уровне приложения. Методология анализа рисков на уровне организации может не подойти для этой задачи.

Ниже приведены примеры вопросов, задаваемых в ходе выполнения высокоуровневого анализа рисков приложения и направленных на определение спецификаций и контекстов приложений.

Примеры

1 Применяется ли приложение только внутренними пользователями или используется через Интернет?

2 Это веб-приложение или приложение для ПК?

3 Обрабатывает ли приложение данные кредитных карт?

4 Имеется ли в приложении компонент для мобильных устройств?

6.2.6.3.3 Детальный анализ рисков безопасности приложения

Процесс детального анализа рисков выполняется на этапе реализации жизненного цикла приложения, как приведено в ИСО/МЭК 27034-1:2011 (подпункт 8.2.2.2).

Этот процесс более точно определяет связанные с приложением остаточные риски перед рассмотрением любых элементов управления безопасностью приложения и подтверждает целевой уровень доверия приложения, определенный в ходе высокоуровневого анализа рисков с учетом подробных спецификаций приложения и технологических особенностей организации, а также регулятивного контекста и бизнес-контекста.

В результате детального анализа рисков владелец приложения может изменить целевой уровень доверия приложения для проекта приложения, тем самым изменив МОБП для проекта. В результате изменятся вовлеченные действующие субъекты и оценочная стоимость проекта. Однако последствия обновления МОБП для безопасности легко прогнозируются, поскольку такая информация, как действующие субъекты, профессиональная квалификация и оценочная стоимость, уже являются частью каждой МОБП, они задокументированы в библиотеке МОБП организации.

Владелец конкретного проекта приложения должен четко определить роль с обязанностью проводить этот анализ с помощью адекватной методологии на уровне приложения. Методология анализа рисков на уровне организации может не подойти для этой задачи.

Ниже приведены примеры вопросов, задаваемых в ходе выполнения детального анализа рисков для приложения.

Пример 1 — Предоставляет ли приложение функцию аутентификации, включающую в себя защиту учетных данных?

Пример 2 — Используется ли для аутентификации база данных или Active Directory?

Пример 3 — Поддерживает ли приложение авторизацию на основе ролей?

Пример 4 — Включает ли приложение код JavaScript?

На основе ответов на вопросы, которые задаются в процессе анализа рисков, формулируются требования безопасности. Эти требования безопасности должны быть задокументированы в НСП (подробнее см. подраздел 6.3). Например:

Пример 5 — Если приложение предоставляет функцию аутентификации на основе форм (учитывается ответ на вопрос в ходе анализа рисков), то функция аутентификации должна быть защищена от атак перебора пользователей (это часть требований безопасности приложения).

6.2.6.3.4 Методы детального анализа рисков приложений

Организация может включить в свою НСО определенные общеизвестные методики, примеры которых приведены ниже.

6.2.6.3.4.1 Моделирование угроз

Моделирование угроз используется в средах, где существует значительный риск безопасности. Такая практика позволяет проектным группам структурированным образом анализировать, документировать и обсуждать последствия применения угроз с целью обеспечения безопасности проектов в контексте их планируемой среды эксплуатации. Моделирование угроз также позволяет учитывать риски безопасности на уровне компонентов или приложения.

Моделирование угроз выполняется группой, включающей в себя руководителей программ/проектов, разработчиков и тестировщиков, и является основной задачей анализа безопасности, выполняемой на этапе разработки программного обеспечения.

6.2.6.3.4.2 Анализ модели угроз и поверхности атаки

Обычно приложение отклоняется от функциональных и проектных спецификаций, определенных на этапах формулирования требований и проектирования. В результате проектные группы должны пересмотреть модели угроз и результаты анализа поверхности атаки определенного приложения, когда код будет готов. Такой пересмотр гарантирует, что любые изменения в проекте или реализации были учтены, и что любые новые векторы атак, появившиеся в результате изменений, были рассмотрены и минимизированы. Модель угроз и процесс пересмотра поверхности атаки могут привести к изменению целевого уровня доверия приложения.

Для проектных команд, которые используют каскадную модель разработки, такой пересмотр выполняется после этапа реализации или после внесения серьезных изменений. В модели гибкой разработки (Agile) это действие должно выполняться на каждой итерации модели.

6.2.6.4 Анализ рисков, связанных с приложением

Согласно ИСО/МЭК 27005 «оценивание рисков основывается на понимании рисков, полученном при анализе рисков, и используется при принятии решений о будущих действиях». Решения должны включать в себя следующее:

a) необходимость в какой-либо процедуре;

b) приоритеты при обработке рисков с учетом установленных значений уровней рисков.

В настоящем стандарте данный этап заключается в выборе целевого уровня доверия приложения, который, в свою очередь, определяет, какие меры обеспечения безопасности приложений необходимо применить для обработки рисков.

В результате оценки рисков владелец приложения может изменить целевой уровень доверия приложения, определенный для проекта приложения. Применяемые МОБП, выбранные для проекта, будут изменены, что повлияет на вовлеченных действующих субъектов и оценочную стоимость проекта.

6.2.6.5 Мероприятия по оценке рисков, связанных с безопасностью приложений

Основные действия, которые организации могут выполнять в ходе оценки рисков безопасности приложений, включают в себя:

a) получение необходимой информации от НСП. Эта информация, обычно предоставляемая на первом этапе ПМБП, должна включать в себя:

1) требования приложения;

2) среду приложения:

i) бизнес-контекст;

ii) регулятивный контекст;

iii) технологический контекст;

3) информацию, полученную, сохраненную, обработанную или предоставленную приложением;

4) категорию безопасности для этой информации;

5) поток этой информации в приложении;

6) определение критической для организации информации;

7) спецификации, функции и компоненты приложения, а также информацию, с которой они работают;

8) процессы приложения, процессы организации, взаимодействующие с приложением, и информацию, с которой они работают;

9) действующие субъекты, вовлеченные в эти спецификации и процессы;

b) категоризация спецификаций, процессов и действующих субъектов в соответствии с категоризацией информации, с которой они работают (они наследуют категории информации);

c) определение критических спецификаций, процессов и действующих субъектов;

d) определение угроз для критической информации на основе среды приложения и критических спецификаций, процессов и действующих субъектов (подпункт 6.2.6.3.4);

e) определение уязвимостей на основе среды приложения и критических спецификаций, процессов и действующих субъектов;

f) определение влияния на организацию на основе внутренней и эксплуатационной ценности критической информации в приложении;

g) определение рисков безопасности приложения на основе собранной выше информации; определение приемлемых и неприемлемых рисков на основе критериев организации;

h) определение стратегии по снижению этих рисков;

i) для каждого неприемлемого риска необходимо определить предпочтительную стратегию снижения, например: обработку, перенос, допущение или прекращение;

j) для каждого неприемлемого риска необходимо определить требования безопасности приложения.

6.2.6.6 Требования безопасности приложений

В большинстве проектов приложений риски безопасности должны учитываться после того, как требования к проекту выполнены, чтобы убедиться, что итоговые требования безопасности также учитывают риски безопасности, возникающие из требований к проекту (например, функциональные требования). После определения эти требования безопасности могут создать процесс обратной связи и повлиять на требования к проекту приложения. Снижение рисков безопасности оказывается дешевле, если это сделано на этапе проектирования и до реализации кода.

Цель определения требований безопасности состоит в том, чтобы четко понять, каких результатов следует ожидать от МОБП, которые будут реализованы для снижения риска до приемлемого уровня.

Основное различие между требованиями к программному обеспечению (или системными требованиями) и требованиями безопасности заключается в том, что требования к программному обеспечению и системам устанавливаются для удовлетворения потребностей (т. е. потребности организаций, пользователей или приложения), а требования безопасности устанавливаются для минимизации рисков.

Требования безопасности должны также определить, как безопасно внедрить и развернуть все функциональные возможности, предоставляемые конкретной функцией. Проектная группа должна проверить проектные спецификации на соответствие функциональной спецификации приложения. Эта группа должна обеспечивать сквозное покрытие, включающее в себя устройства, которые обращаются к системе приложения, межсистемным интерфейсам и любым внешним соединениям.

Определение точных и надежных требований безопасности, охватывающих все риски, которым подвержено приложение, бывает затруднено. В рекомендациях, приведенных далее, предлагается специальная таксономия, которую некоторые организации могут найти полезной.

Тип требований безопасности приложений определяется путем идентификации действующего субъекта, к которому относится это требование. Например, если требование безопасности указывает, что пользователь должен ввести пароль, это требование будет определено как требование к пользователю. Если требование безопасности предписывает, что приложение должно вести журнал определенных критических транзакций, это требование будет определено как системное требование.

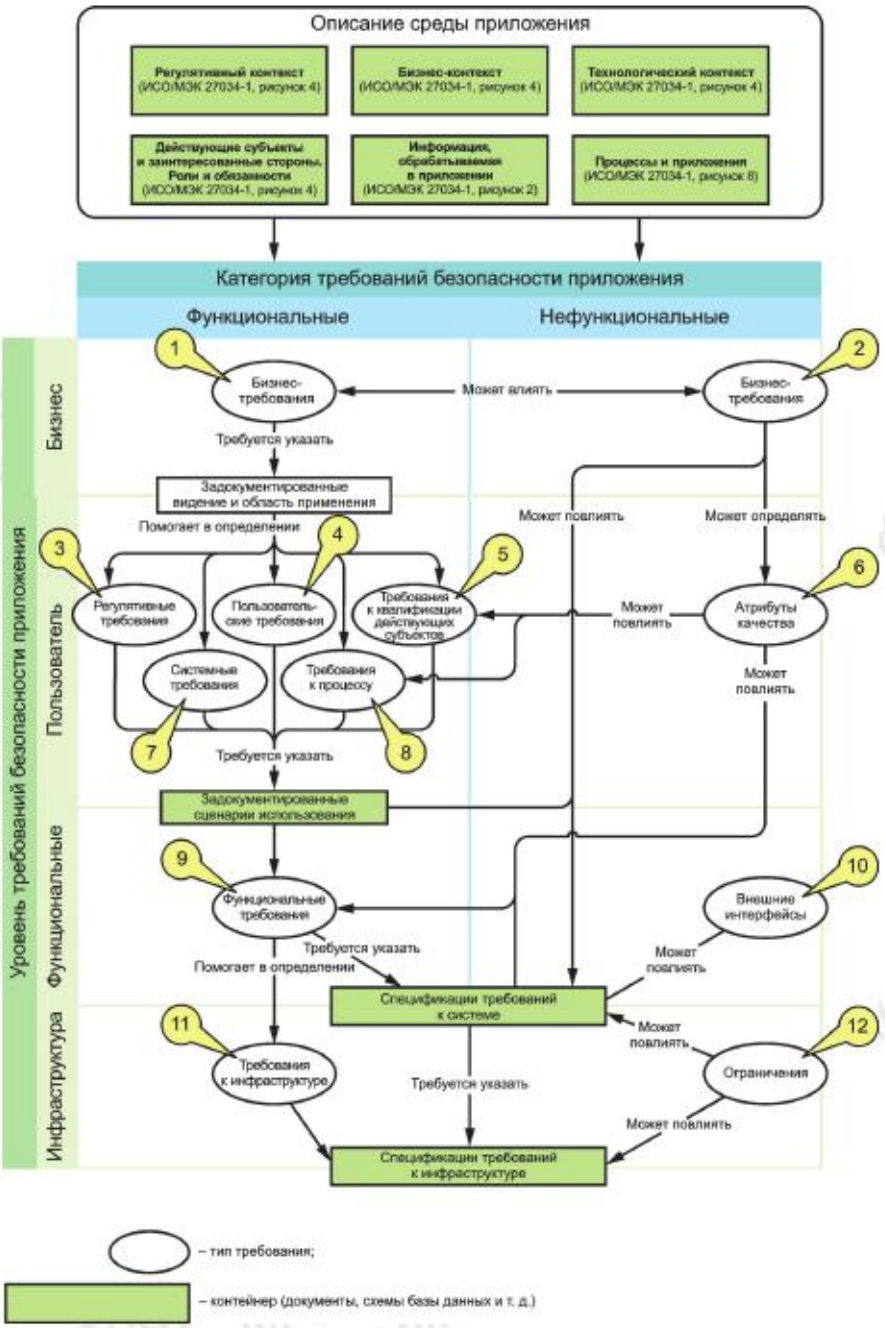

Рисунок 5 — Типы требований безопасности приложения

Как показано на рисунке 5, требования безопасности, как и требования к программному обеспечению, могут быть разделены на две категории (функциональные и нефункциональные), четыре уровня (бизнес, пользователи, функции и инфраструктура), а также 12 типов:

a) Бизнес-требования. Требование обеспечения безопасности бизнеса направлено на устранение как минимум одного риска для обеспечения безопасности из бизнес-контекста организации, такого как: практики, цели организации, информация для защиты целевой клиентуры и т. д.

b) Бизнес-правила. Правило обеспечения безопасности бизнеса устраняет по крайней мере одну угрозу безопасности из правил работы организации, таких как директивы, внутренние правила, кодексы поведения и т. д.

c) Регулятивные требования. Регулятивное требование направлено как минимум на один риск для обеспечения безопасности из регулятивного контекста, которому подвержена организация.

d) Пользовательские требования. Пользовательское требование устраняет по крайней мере одну угрозу безопасности от действий, которые могут быть выполнены субъектом (менеджером, членом технической группы, оператором, пользователем, слушателем) во время работы с приложением.

e) Требования к квалификации. Требования к квалификации к безопасности направлено на устранение как минимум одного риска безопасности из ограничений или квалификаций до того, как действующему субъекту будет разрешено выполнить действие в среде разработки или среде эксплуатации приложений. Этот тип требований может применяться к субъекту или системному компоненту.

Примеры

1 Прежде чем получить разрешение на разработку нового компонента Java, разработчик должен доказать необходимую квалификацию и знания, например предоставить диплом/сертификат, подтвердить минимальное количество лет опыта.

2 Прежде чем компонент приложения будет развернут в среде, он должен быть сертифицирован как способный обнаруживать и реагировать на распределенные атаки типа «отказ в обслуживании», попытки несанкционированного изменения данных или сбои другого компонента системы.

f) Атрибуты качества. Атрибут качества учитывает, по крайней мере, один риск безопасности, связанный с недостижением целей в области качества приложения (возможность повторного использования, удобство использования, целостность, переносимость, совместимость, возможность обслуживания и т. д.).

g) Системные требования. Системное требование безопасности направлено как минимум на одну угрозу безопасности со стороны услуг и функций, предлагаемых приложением.

h) Требования к процессу. Требование к безопасности процесса направлено на устранение как минимум одного риска безопасности, вызванного или затронутого какими-либо процессами внедрения или эксплуатации (процессы разработки, развертывания, делегирования, использования, обслуживания и архивирования, а также непредвиденные обстоятельства.

i) Функциональные требования. Требование к функциональной безопасности учитывает как минимум один риск безопасности, связанный с функциями, предлагаемыми системой (онлайн-платежи, передача данных, корзина покупок, удаленное управление и т. д.).

j) Внешние интерфейсы. Требование к безопасности внешнего интерфейса устраняет по крайней мере одну угрозу безопасности, исходящую от различных интерфейсов, предлагаемых системой (веб-интерфейсы и интерфейсы связи с другими приложениями).

k) Требования к инфраструктуре. Требование к безопасности инфраструктуры направлено как минимум на один риск безопасности, исходящий от среды физической инфраструктуры, которая поддерживает приложение.

l) Ограничения. Ограничение безопасности устраняет по крайней мере одну угрозу безопасности, исходящую от ограничений, наложенных на приложение или требуемых для него. Например, приложение должно быть доступно через Интернет, не должен разрабатываться на Java какой-либо компонент приложения, или конкретное действие может быть выполнено только при одновременном действии двух игроков. Ограничения могут описывать количественные критерии, такие как требуемая производительность, время зарядки или время отклика для нескольких сайтов, а также качественные ограничения, такие как удобство обслуживания и удобство пользования.

Для максимальной ясности требование безопасности должно включать в себя по крайней мере следующие элементы:

a) роль действующего субъекта, который должен выполнить действие (кто);

b) желаемое действие по снижению риска (как);

c) момент, в который действие должно быть выполнено (когда);

d) где это действие должно быть выполнено (где);

e) информация, затрагиваемая этим требованием (что);

f) риск или источник риска, к которому относится это требование безопасности (почему).

Точно так же, как МОБП может быть представлено в графическом виде (см. ИСО/МЭК 27034-1:2011, рисунок 7), общие или высокоуровневые требования безопасности должны генерировать набор более конкретных требований.

Чтобы ускорить разработку, требование безопасности, разработанное во время реализации проекта приложения, может быть заменено эквивалентным требованием безопасности (снижающим тот же риск до приемлемого для проекта уровня), который уже присутствует в НСО. Библиотека МОБП организации содержит информацию, связывающую риски, требования и меры обеспечения безопасности [см. ИСО/МЭК 27034-2:2015 (пункт 5.5.7)].

В ходе разработки программного обеспечения проверка выполнения требований часто вызывает затруднения. Гораздо проще проверить, что соблюдены требования безопасности приложения. Для достижения каждого требования выбирается одно или несколько МОБП, как приведено на рисунке 3. Проверка правильности реализации этих МОБП гарантирует выполнение требования.

6.2.6.7 Определение целевого уровня доверия приложения

После того, как анализ рисков безопасности приложения завершен, а требования безопасности определены и проверены, целевой уровень доверия приложения должен быть идентифицирован с использованием библиотеки МОБП организации. Эта идентификация должна быть выполнена путем сравнения требований к безопасности, разработанных для приложения, с требованиями безопасности, перечисленными в библиотеке МОБП организации. Когда два требования безопасности почти идентичны (снижение одного и того же риска безопасности до одного и того же приемлемого уровня), можно заменить требование безопасности, определенное для приложения, на то, которое присутствует в библиотеке МОБП. Это гарантирует, что схожие требования безопасности всегда будут выполняться одинаковыми МОБП.

Если требование безопасности, определенное для приложения, не имеет эквивалента в библиотеке МОБП, запрос МОБП, который может включать в себя предложение МОБП, должен быть отправлен в группу НСО посредством процесса «Мониторинг и проверка НСО» [см. ИСО/МЭК 27034-2:2015 (пункт 5.4.6)].

Как только все требования безопасности, определенные для приложения, сопоставлены с теми, которые присутствуют в библиотеке МОБП, идентификатором требуемого целевого уровня доверия приложения для этого приложения будет уровень доверия приложения, который включает в себя как минимум все требования безопасности.

Затем проектная группа приложения должна подготовиться к передаче приложения владельцу для утверждения:

a) списка рисков безопасности и связанных с ними последствий, оцененных для данного проекта приложения;

b) списка требований безопасности для адекватной минимизации этих угроз безопасности;

c) уровня доверия приложения, включающего в себя МОБП, отвечающие требованиям безопасности, которые должны быть выполнены для этого приложения.

Проектная группа должна представить эту и другую вспомогательную информацию таким образом, чтобы помочь владельцу приложения принять обоснованное решение.

Пример — Группа может показать связи между рисками/требованиями безопасности, МОБП и затратами в табличной или графической форме, чтобы помочь владельцу приложения понять последствия и стоимость снижения каждого риска до приемлемого уровня и утверждения целевого уровня доверия приложения.

6.2.6.8 Принятие владельцем приложения

Владелец приложения несет ответственность за принятие остаточных рисков, связанных с определенным приложением, после их оценки. Данный этап соответствует этапу «принятие риска информационной безопасности» в рамках процесса менеджмента рисков, приведенного в ИСО/МЭК 27005.

Владелец может сделать это двумя способами:

a) утвердив целевой уровень доверия приложения на шаге 2 ПМБП;

b) утвердив результаты шага 5 ПМБП, в котором измеряется фактический уровень доверия приложения и сравнивается с целевым уровнем доверия приложения. Владелец приложения может прибегнуть к этому шагу в любое время.

Для дополнительного подтверждения владелец приложения может потребовать выполнения этого шага внешней группой, осуществляющей верификацию.

Ниже приведен пример остаточного риска, который может быть принят владельцем приложения.

Пример — Разрешить функцию «запомнить меня» на странице входа в приложения, используемые внутренними пользователями.

В приведенном выше примере владелец приложения подтверждает, что уровень риска, связанный с функцией «запомнить меня» для внутренних приложений, приемлем. Функция «запомнить меня» представляет такие риски, как несанкционированный доступ к приложению, если злоумышленник получит физический доступ к разблокированной рабочей станции жертвы. Владелец приложения может принять этот риск, учитывая, что вероятность такого несанкционированного физического доступа во внутреннем офисе организации невысока.

После того, как владелец принял остаточные риски, проектная группа берет на себя ответственность за достижение целевого уровня доверия приложения путем внедрения соответствующих МОБП на соответствующих этапах жизненного цикла.

6.3 Создание и поддержка нормативной структуры приложения

6.3.1 Общие положения

На третьем этапе ПМБП происходит выбор всех элементов НСО, которые применяются к конкретному проекту приложения, и формирование НСП для этого приложения. Процесс формирования НСП для конкретного приложения является обязательным. Как показано на рисунке 6, НСП является подмножеством или уточнением НСО и содержит только применимую информацию для конкретного приложения, включая целевой уровень доверия приложения, требуемые МОБП, контексты приложения (бизнес-контекст, регулятивный и технологический контексты), обязанности и профессиональную квалификацию действующих субъектов, а также спецификации приложения. Эта информация определяется или генерируется на этапах 1 и 2 ПМБП, документируется и хранится в НСП.

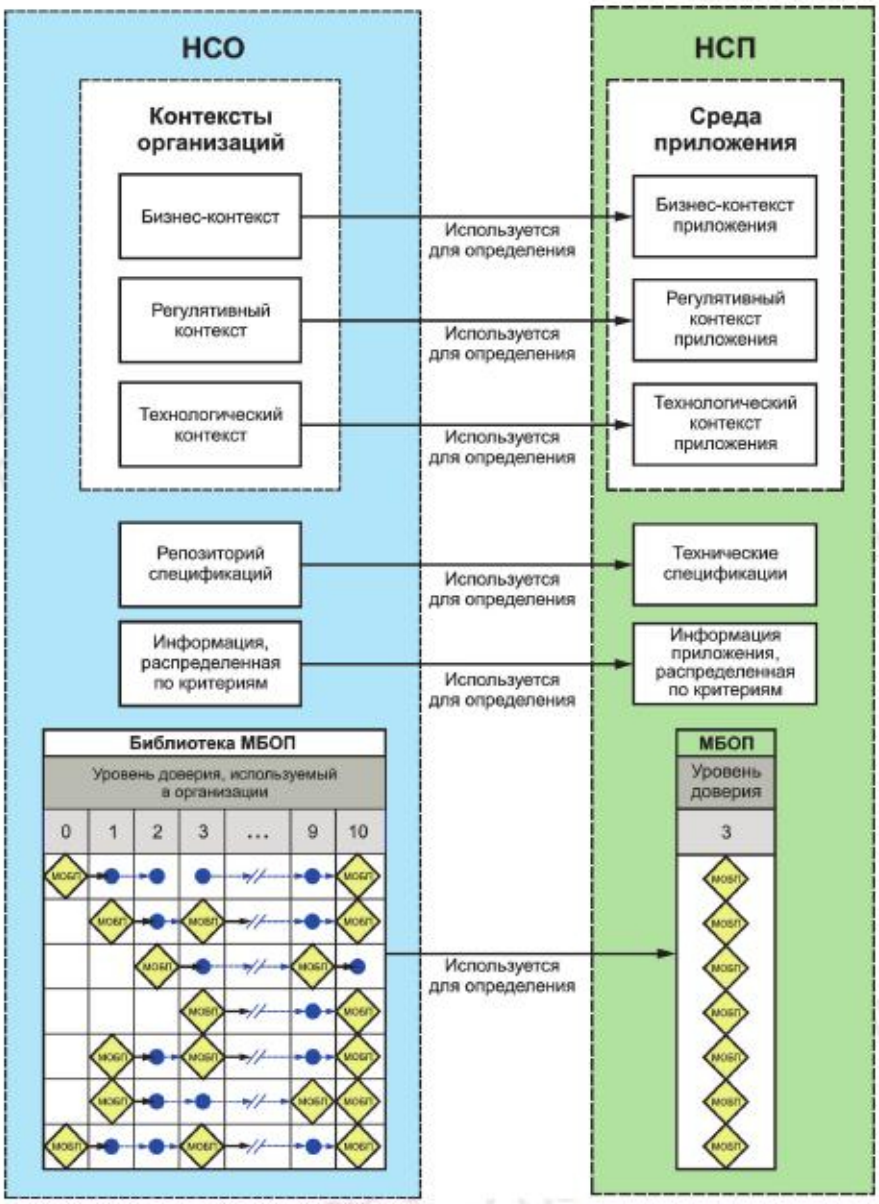

Рисунок 6 — Создание НСП на основе НСО

На данном этапе организация должна определить жизненный цикл приложения для проекта приложения. Жизненный цикл приложения является подмножеством эталонной модели жизненного цикла безопасности приложения [см. ИСО/МЭК 27034-1:2011 (подпункт 8.1.2.7)] в НСО. Жизненный цикл для конкретного проекта будет содержать только процессы, необходимые для проекта приложения.

Например, проект, разрабатываемый внутри организации, не будет включать в себя процессы, связанные с аутсорсингом.

Данный этап также выполняется для проверки того, что соответствующие элементы НСО, которые применяются к конкретному проекту приложения, должным образом зарегистрированы в нормативной структуре приложения (НСП).

Примечания

1 Данный этап соответствует этапу «обработка риска информационной безопасности» в рамках процесса менеджмента рисков, приведенного в ИСО/МЭК 27005.

2 Жизненный цикл приложения для проекта приложения получен из соответствующей модели жизненного цикла безопасности приложения, хранящейся в НСО. Модель жизненного цикла приложения представляет собой сопоставление элементов ЭМЖЦБП с конкретными методами или процессами в организации, такими как процесс аутсорсинга, процесс приобретения, процесс разработки (например, RUP[1], RAD[2]), процесс эксплуатации и управления (например, SCRUM), процесс управления и обслуживания ИТ (например, ITIL[3]) [см. ИСО/МЭК 27034-2:2015 (пункт 5.5.10)].

6.3.2 Назначение

Целями данного этапа являются управление и поддержание содержимого НСП в течение жизненного цикла конкретного приложения путем пересмотра, проверки, импорта и консолидации значимых элементов из НСО, включая:

a) МОБП, определяемые целевым уровнем доверия приложения;

b) информацию, генерируемую на разных этапах ПМБП;

c) жизненный цикл приложения.

Примечание — Данный этап соответствует шагу «подготовка и реализация планов по обработке рисков» в рамках этапа «обработка рисков» в процессе менеджмента рисков, приведенном в ИСО/МЭК 27005.

6.3.3 Результаты

Основные результаты данного этапа включают в себя:

a) обновленную и выпущенную полную НСП, содержащую все необходимые элементы для защиты приложения;

b) жизненный цикл приложения для проекта приложения;

c) применимые МОБП для проекта приложения.

6.3.4 Мероприятия по реализации

В таблице 7 показаны роли и обязанности по выполнению действий по реализации процесса «Создание и поддержка нормативной структуры приложения».

Таблица 7 — Диаграмма RACI для процесса «Создание и поддержка нормативной структуры приложения»

Мероприятия по реализации	Менеджер проекта	Проектная группа	Владелец приложения
1) Определение и выбор процессов и ключевых действий из НСО для создания НСП	A	R	C
2) Проверка соответствия внутренних моделей жизненного цикла безопасности приложения, используемых в этом проекте приложения, соответствующим этапам и действиям ЭМЖЦБП	A	R	C
3) Импортирование в НСП требуемых процессов и МОБП, определяемые уровнем доверия приложения, присвоенным приложению	R	I	A
4) Поддержка и передача НСП заинтересованным сторонам	A	R	I

6.3.5 Мероприятия по верификации

В таблице 8 показаны роли и обязанности по выполнению действий по верификации процесса «Создание и поддержка нормативной структуры приложения».

---

[1] *Методология разработки программного обеспечения (методология RUP).*

[2] *Методология разработки программного обеспечения (методология RAD).*

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

Таблица 8 — Диаграмма RACI для верификации процесса «Создание и поддержка нормативной структуры приложения»

Мероприятия по верификации	Проектный менеджер	Аудиторы
1) Подтверждение того, что нормативная структура приложения была определена	I	A/R
2) Подтверждение того, что жизненный цикл приложения для проекта приложения сформирован	I	A/R
3) Подтверждение того, что были выбраны меры обеспечения безопасности для проекта приложения	I	A/R
4) Подтверждение того, что содержание НСП было проверено и подписано владельцем приложения	I	A/R

6.3.6 Рекомендации

6.3.6.1 Общие положения

Действия, необходимые для обеспечения эффективного определения требований и среды приложения, включают в себя:

a) формирование НСП.

Информация из НСО, которая влияет на проект разработки приложения, должна быть записана в НСП.

Эта информация должна включать в себя, по крайней мере: целевой уровень доверия приложения, контекст приложения (бизнес-контекст, регулятивный и технологический контексты), обязанности и профессиональные квалификации участников, спецификации приложения, требования к дизайну, а также процессы, связанные с определением, управлением и проверкой безопасности приложения.

НСП для проекта приложения развивается в течение всего жизненного цикла приложения. На начальном этапе проекта приложения формируется начальная НСП. Эта начальная НСП совершенствуется по мере того, как в рамках проекта приложения накапливается больше знаний;

b) формирование жизненного цикла приложения.

Эталонная модель жизненного цикла безопасности приложения (ЭМЖЦБП), содержащаяся в НСО, должна быть проанализирована с целью определения жизненного цикла приложения для проекта приложения. Это означает, что экземпляр ЭМЖЦБП формируется и трансформируется в специализированный жизненный цикл безопасности приложения, который содержит необходимую подробную информацию (процессы) для проекта приложения;

c) выбор мер обеспечения безопасности для проекта приложения МОБП, которые копируются из НСО в НСП.

На основе целевого уровня доверия приложения, потребностей организации в отношении приложения, а также конкретных условий и спецификаций приложения следует выбирать применимые меры обеспечения безопасности для проекта приложения.

Примечание — МОБП могут быть обновлены для этого приложения только с разрешения владельца приложения и группы НСО;

d) обеспечение того, чтобы требования безопасности приложения были определены с учетом подтверждающих документов, таких как нормативные требования или спецификации программного обеспечения;

e) обеспечение того, чтобы потоки информации были детализированы;

f) определение бизнес-контекста, технологического и регулятивного контекстов приложения;

g) определение того, были ли участники вовлечены в процесс реализации;

h) подтверждение того, что вся полученная актуальная информация была записана в целях создания НСП;

i) сохранение результатов процесса верификации в НСП.

Должна быть выполнена верификация компонентов в НСП:

a) перед ключевыми этапами в проекте приложения;

b) в случае изменения бизнес-контекста, технологического или регулятивного контекстов;

c) в ходе периодических аудитов.

Рекомендуется, чтобы ответственность за проверку НСП описывалась в диаграмме RACI, аналогичной таблице 8.

6.3.6.2 Процессы обеспечения безопасности приложений

Значимые процессы, связанные с определением, управлением и проверкой безопасности приложений, должны быть включены в НСП. Эти процессы относятся к компоненту «процессы, связанные с безопасностью приложений» НСО. Некоторыми примерами таких процессов являются процедуры анализа уязвимостей, процедуры анализа исходного кода, планы реагирования на инциденты и т. д.

Чтобы обеспечить полноту, актуальность и точность НСП для конкретного приложения, рекомендуется определить обязанности для различных компонентов НСП.

6.3.6.3 Процессы, связанные с НСП

Организация должна определить и задокументировать процессы создания, утверждения и поддержания НСП. Должны быть указаны роли, обязанности и требуемая профессиональная квалификация действующих субъектов, вовлеченных в НСП организации для конкретного приложения. МОБП, указанные в нормативной структуре организации (НСО), связаны с этапами эталонной модели жизненного цикла безопасности приложения, а МОБП, указанные в нормативной структуре приложений (НСП), — с этапами жизненного цикла конкретного проекта приложения.

В ИСО/МЭК 27034-1:2011 (подпункт 8.1.2.7.1) указано, что необходимо обеспечивать соответствие между процессами в эталонной модели жизненного цикла безопасности приложений и процессами в каждом жизненном цикле, используемом в организации.

Процесс создания НСП определяет конкретный жизненный цикл безопасности приложения для проекта приложения путем выбора значимых процессов и действующих субъектов из НСО. В процессе создания НСП также выбираются МОБП из библиотеки МОБП в соответствии с целевым уровнем доверия приложения, принятым владельцем приложения.

Организации должны провести валидацию НСП, после чего НСП должна быть подписана владельцем приложения.

6.4 Подготовка к работе и эксплуатация приложений

6.4.1 Общие положения

Четвертый этап ПМБП включает в себя использование МОБП, сформированных на основе НСП, для конкретного приложения в течение его жизненного цикла. Например, организация может принять решение о разработке, приобретении и (или) эксплуатации приложения. Данный этап ПМБП следует применять как к этапам подготовки в жизненном цикле приложения, так и к этапам эксплуатации, он помогает интегрировать МОБП, определенные в соответствии с целевым уровнем доверия приложения, в любые существующие процессы или компоненты приложения. Данный этап также включает в себя проверку того, что все действия МОБП были интегрированы в жизненный цикл приложения.

На данном этапе проектной группе и группе проверки предоставляются МОБП, связанные с целевым уровнем доверия приложения для их проекта.

МОБП также используются группой проверки, поскольку они предоставляют подробную информацию о том, какие измерения должны быть проведены, чтобы предоставить доказательство того, что действия по обеспечению безопасности были выполнены правильно и дали ожидаемые результаты.

Ключевые действующие субъекты, которые могут обеспечивать меры безопасности из МОБП, приведены на рисунке 7.

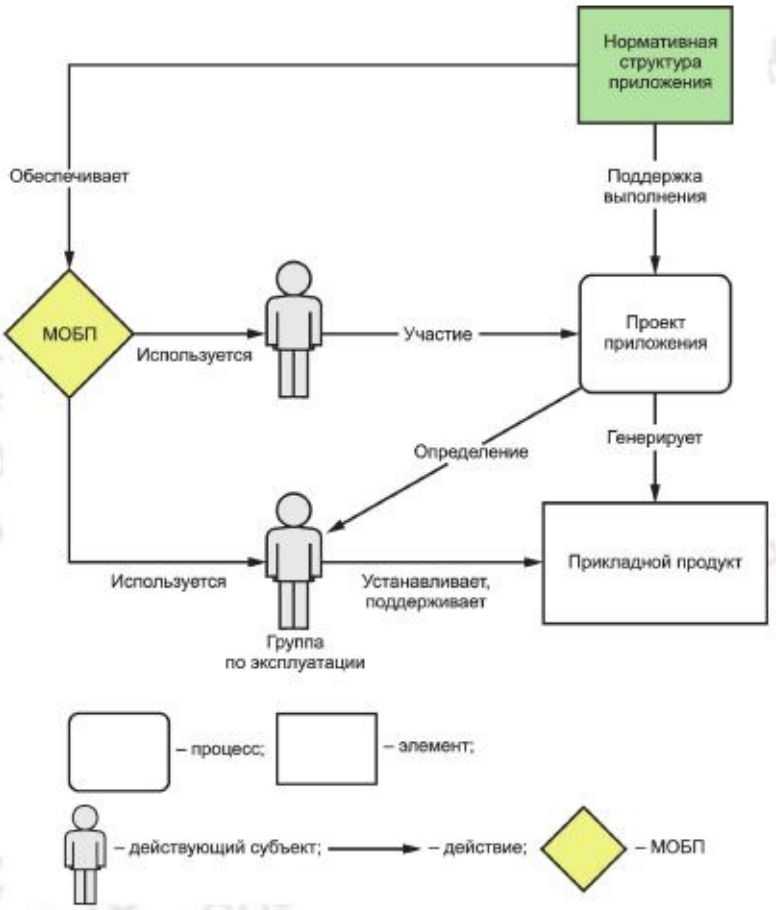

Рисунок 7 — МОБП, используемые для действий по обеспечению безопасности

Менеджеры проектов должны найти в МОБП подробную информацию, такую как требуемые задачи, ресурсы и квалификации, трудоемкость выполнения в человеко-днях и конкретный этап жизненного цикла, на котором должна выполняться каждая задача.

Примечание

1 Данный этап соответствует этапу «обработка риска информационной безопасности» в рамках процесса менеджмента рисков, приведенного в ИСО/МЭК 27005.

2 Защищенные системы управления жизненным циклом приложений могут дополнительно использоваться проектными группами и группами проверки для управления и отслеживания действий по обеспечению безопасности, приведенных в МОБП, в течение всего жизненного цикла приложения.

6.4.2 Назначение

Целью реализации этого процесса является создание элементов НСП, относящихся к соответствующим этапам, фазам и действиям, охватываемым проектом.

Проектная группа реализует МОБП из НСП:

a) часть действий по обеспечению безопасности каждой МОБП осуществляется действующим субъектом, указанным в МОБП;

b) часть мер безопасности каждой МОБП осуществляется действующим субъектом, указанным в МОБП.

6.4.3 Результаты

В результате успешного выполнения этого процесса должна быть получена следующая информация:

a) список выполненных МОБП и результаты их выполнения;

b) артефакты приложения, в том числе обновленная НСП;

c) обратная связь с процессом управления НСО, если это применимо;

d) сведения о любых различиях между целевым и фактическим уровнем доверия приложения в результате выполнения этапа 5;

e) отчеты и результаты аудита каждой МОБП приложения, включая, в частности, объем аудита, состояние каждой МОБП, недостатки и возможные решения для их устранения, в том числе:

1) результаты выполнения мероприятий по обеспечению безопасности из МОБП, связанных с целевым уровнем доверия приложения для проекта приложения;

2) результаты измерений с целью верификации, выполненных с использованием МОБП в проекте;

f) фактический уровень доверия приложения для приложения, как результат этапа 5;

g) прототип приложения (функциональное подмножество приложения) или приложение целиком, в зависимости от итерации в жизненном цикле, с соответствующими МОБП, реализованными и проверенными.

6.4.4 Мероприятия по реализации

Роли и обязанности по выполнению действий по реализации процесса «Подготовка и эксплуатация приложения» приведены в таблице 9.

Таблица 9 — Диаграмма RACI для процесса «Подготовка и эксплуатация приложения»

Мероприятия по реализации	Менеджер проекта	Проектная группа	Владелец приложения	Аудиторы
1) Проведение подробного анализа рисков безопасности приложения	A/R	R	C	I
2) Принятие мер по обеспечению безопасности в рамках каждой МОБП	A	R	I	I
3) Выполнение мероприятий по верификации в рамках каждой МОБП	C	C	I	A/R
4) Предоставление обратной связи процессу менеджмента НСО по мере необходимости	A/R	I	I	I

6.4.5 Мероприятия по верификации

Роли и обязанности по выполнению действий по верификации процесса «Подготовка и эксплуатация приложения» приведены в таблице 10.

Таблица 10 — Диаграмма RACI для верификации процесса «Подготовка и эксплуатация приложения»

Мероприятия по верификации	Менеджеры	Аудиторы
1) Подтверждение того, что в организации имеется список действий по обеспечению безопасности в рамках МОБП, связанных с целевым уровнем доверия приложения для проекта приложения	I	A/R
2) Гарантия выполнения действий по обеспечению безопасности из этого списка	I	A/R
3) Подтверждение того, что в организации имеется список верификационных измерений, который входит в состав МОБП	I	A/R
4) Гарантия выполнения измерений из этого списка	I	A/R
5) Подтверждение того, что прототип приложения с соответствующими МОБП был реализован и верифицирован	I	A/R

6.4.6 Рекомендации

6.4.6.1 Общие положения

Если в ходе выполнения данного этапа ПМБП, например, при детальном анализе рисков или разработке детальной архитектуры, проектная группа определит, что МОБП в НСП необходимо адаптировать, исправить или иным образом изменить или что новые МОБП необходимы для надлежащего удовлетворения требований безопасности приложения, она должна сообщить об этом посредством процесса управления НСО, чтобы необходимые изменения были выполнены приемлемым для организации способом.

Это взаимодействие обозначено на рисунке 1 в виде стрелки с надписью «Обеспечивает обратную связь с». В ИСО/МЭК 27034-2:2015 (рисунок 1) показано, что это взаимодействие в основном нацелено на подпроцесс «Мониторинг и пересмотр НСО». В ИСО/МЭК 27034-2:2015 (подпункт 5.4.6.5) приведены примеры и указано, что «обратная связь от проектов приложений также должна использоваться в качестве одного из важнейших источников информации для постоянного улучшения качества и эффективности МОБП, применяемых в проектах».

Некоторые организации могут считать приемлемым, что проектные группы предоставляют при использовании обратной связи предложения по обновлению существующих или внедрению новых МОБП, особенно если проектная группа в настоящее время имеет требуемый опыт такой работы. В любом случае новые или обновленные МОБП предоставляются проектным группам организации в результате подпроцесса «Улучшение НСО» процесса управления НСО [см. ИСО/МЭК 27034-2:2015 (подпункт 5.4.7.2)].

Примечание — Некоторые рекомендации по реализации и эксплуатации приложения приведены в приложении А.

6.5 Аудит безопасности приложения

6.5.1 Общие положения

Пятым и последним этапом ПМБП является проверка безопасности приложения, т. е. верификация результатов проверки действий по измерению каждой МОБП, указанной в целевом уровне доверия приложения и подлежащей реализации в приложении. Результаты этих действий по проверке МОБП предоставят доказательства того, что применяемые МОБП на момент проверки применялись, как и ожидалось. Данный этап ПМБП может быть выполнен в любое время в течение жизненного цикла приложения. В зависимости от целевого уровня приложения, этап можно реализовать один раз, периодически или в зависимости от события.

Этот процесс показывает фактический уровень доверия приложения в данный момент. Приложение считается безопасным, когда фактический уровень доверия приложения соответствует целевому уровню доверия приложения, утвержденному владельцем приложения в определенный момент времени, или превышает этот уровень.

Часть МОБП, относящаяся к верификационным измерениям, определяет действия по обеспечению безопасности, которые должны быть проверены, чтобы предоставить доказательства того, что действия были выполнены квалифицированным субъектом правильно и дали ожидаемые результаты.

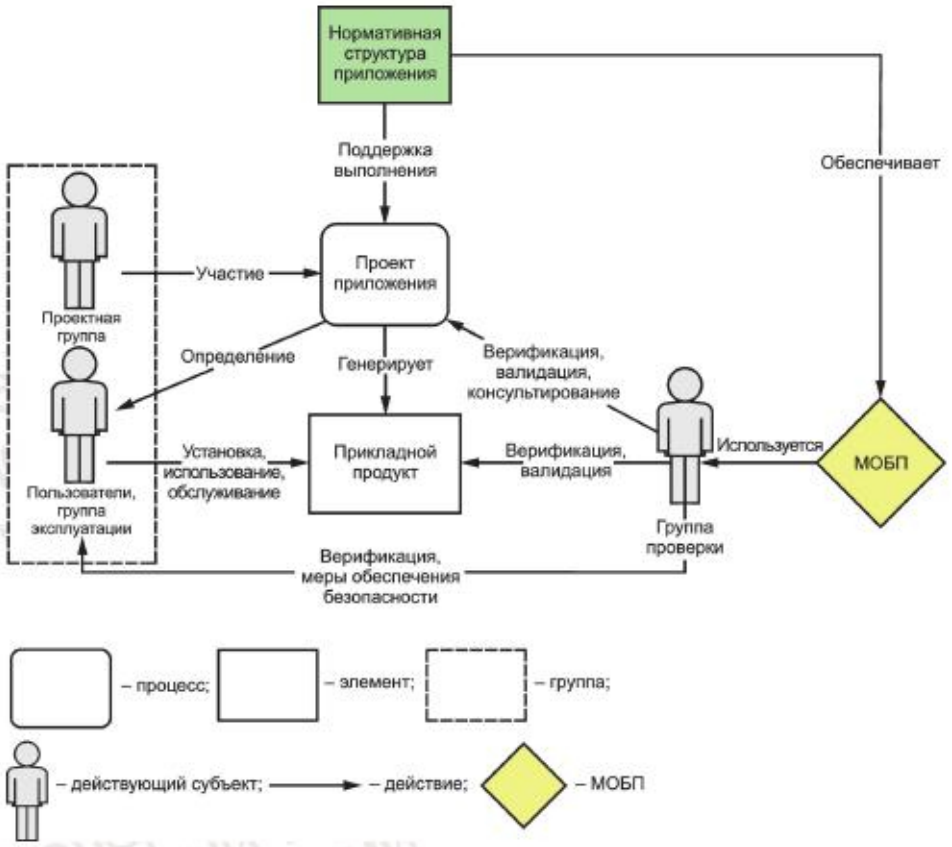

Рисунок 8 — МОБП, используемые для верификационных измерений

На рисунке 8 показано, что часть МОБП, относящаяся к верификационным измерениям, используется командой верификации в качестве контрольной точки для проверки и валидации приложения и проекта, а также для предоставления рекомендаций владельцу приложения, чтобы он мог решить, может ли проект приложения перейти к следующему этапу реализации. Например, МОБП может потребовать использования службы кластеризации серверов для обеспечения доступности приложения. Часть МОБП, относящаяся к верификационным измерениям, подтверждает, что такая служба действительно была реализована.

На рисунке 8 также показано, что часть МОБП, относящаяся к верификационным измерениям, может использоваться для проверки квалификации участников, которые выполняли процессы в жизненном цикле приложения. Например, МОБП может требовать, чтобы критически важный компонент приложения реализовывал старший разработчик. Часть МОБП, относящаяся к верификационным измерениям, проверяет квалификацию разработчика, который внедрил компонент.

К концу данного этапа организация может объявить приложение «безопасным», если его фактический уровень доверия приложения соответствует целевому. Оно сохраняет статус «безопасного» до следующей обязательной проверки, будь то периодическая проверка, требуемая ПМБП, или какая-либо другая проверка, требуемая организацией.

Примечание — Несмотря на название данного этапа, его назначение и описание, приведенные в настоящем стандарте, делают его более тесно связанным с концепцией проверки безопасности приложения, чем с концепцией аудита безопасности приложения (подраздел 3.1). Правильнее было бы назвать данный этап «пере-

смотр безопасности приложения». Однако текущее название сохраняется, чтобы обеспечить согласованность с ИСО/МЭК 27034-1.

6.5.2 Назначение

Целью пятого этапа ПМБП является проверка и официальная регистрация доказательств того, что конкретное приложение достигло целевого уровня доверия приложения в конкретный момент времени и поддерживает этот уровень.

6.5.3 Результаты

Основными результатами данного этапа являются:

a) результаты выполнения процесса пересмотра безопасности приложения, которые демонстрируют, что все верификационные измерения, предоставленные всеми МОБП в НСП для конкретного приложения, были выполнены, и что результаты были верифицированы;

b) фактический уровень доверия приложения в определенное время;

c) доказательство того, что конкретное приложение достигло целевого уровня доверия приложения в определенный момент времени и поддерживает его;

d) результаты проверки и зарегистрированные данные о достижении и поддержании целевого уровня доверия приложения в определенный момент времени.

6.5.4 Мероприятия по реализации

Роли и обязанности по выполнению действий в ходе реализации процесса «Верификация безопасности приложения» приведены в таблице 11.

Таблица 11 — Диаграмма RACI для процесса «Верификация безопасности приложения»

Мероприятия по реализации	Менеджеры	Аудиторы
1) Подтверждение того, что все МОБП, связанные с целевым уровнем доверия приложения, были импортированы в НСП и реализованы в приложении	I	A/R
2) Сравнение фактического уровня доверия приложения с целевым уровнем	I	A/R
3) Документирование доказательства того, что конкретное приложение достигло целевого уровня доверия приложения в определенный момент времени и поддерживает его	I	A/R
4) Подтверждение того, что мероприятия по проверке наличия МОБП в НСП были выполнены, и ожидаемые результаты были получены и верифицированы	I	A/R
5) Измерение фактического уровня доверия приложения	I	A/R

6.5.5 Мероприятия по верификации

В таблице 12 показаны роли и обязанности по выполнению процесса «Верификация безопасности приложения».

Таблица 12 — Диаграмма RACI для процедур верификации в рамках процесса «Верификация безопасности приложения»

Мероприятия по верификации	Менеджеры	Аудиторы
1) Подтверждение того, что результаты процесса проверки безопасности приложения демонстрируют, что все верификационные измерения, предоставленные всеми МОБП в НСП для конкретного приложения, были выполнены, и результаты были верифицированы	I	A/R
2) Подтверждение того, что фактический уровень доверия приложения в определенное время был измерен	I	A/R
3) Обеспечение информирования о том, что конкретное приложение достигло целевого уровня доверия приложения в определенный момент времени и поддерживает его	I	A/R
4) Подтверждение того, что результаты верификации и данные о достижении и поддержании целевого уровня доверия приложения в определенный момент времени были задокументированы	I	A/R

6.5.6 Рекомендации

Для организации этот процесс используется для определения того, что элементы НСО, идентифицированные уполномоченным органом, были реализованы и успешно прошли процесс верификации.

Для приложения этот процесс используется для определения того, что все МОБП, заданные целевым уровнем доверия приложения, были реализованы и успешно прошли процесс верификации.

Данный этап может быть выполнен внутренней или внешней группой верификации. Внутренние аудиты, иногда называемые аудитами первой стороны, проводятся самой организацией или от ее имени. Это анализ проводится с целью подготовки отчета для руководства или достижения других внутренних целей (например, с целью подтверждения эффективности системы управления или получения информации для улучшения процесса управления НСО). Внутренние аудиты могут послужить основой для самостоятельного подтверждения организацией соответствия НСО или требованиям приложения.

Внешние аудиты включают в себя аудиты второй стороны и аудиты третьей стороны. Аудиты второй стороны проводятся сторонами, заинтересованными в организации, такими как правительство, клиенты, поставщики или другие лица, действующие от их имени.

Аудиты третьей стороны проводятся независимыми аудиторскими организациями, такими как регулирующие органы и организации по сертификации.

Чтобы убедиться, что результаты верификации элементов не были подделаны, аудитор безопасности приложения может выбрать повторную верификацию выбранных элементов в рамках сертификации безопасности приложения.

Определение объема проверки безопасности приложения или аудита часто оказывается проблематичным. ИСО/МЭК 27034 (все части) помогает решить эту проблему: максимальный объем верификации или аудита безопасности приложения составляют действия по верификации из МОБП, содержащихся в НСП приложения.

Группа верификации и группа обеспечения безопасности могут считать концепцию МОБП полезной, поскольку каждая МОБП для конкретного приложения предоставляет подробную информацию о действиях по обеспечению безопасности и соответствующих верификационных измерениях. Согласно ИСО/МЭК 27034-1:2001 (подпункт 8.1.2.6.5.4), процедуры верификации и ожидаемые результаты указываются в разделе «Верификационное измерение» МОБП.

Управление проектами приложений может использовать концепцию МОБП как эффективный инструмент для обеспечения безопасности приложений. МОБП детализирует требуемые задачи верификации, профессиональные ресурсы с определенной квалификацией, примерную трудоемкость, например в человеко-днях для задач верификационного измерения проверки, и точные этапы в жизненном цикле приложения, на которых должно выполняться верификационное измерение.

Этот процесс может также использоваться процессом аудита и сертификации для повторного тестирования МОБП приложения и представляет собой этап «Обработка риска информационной безопасности» в процессе менеджмента рисков в соответствии с ИСО/МЭК 27005.

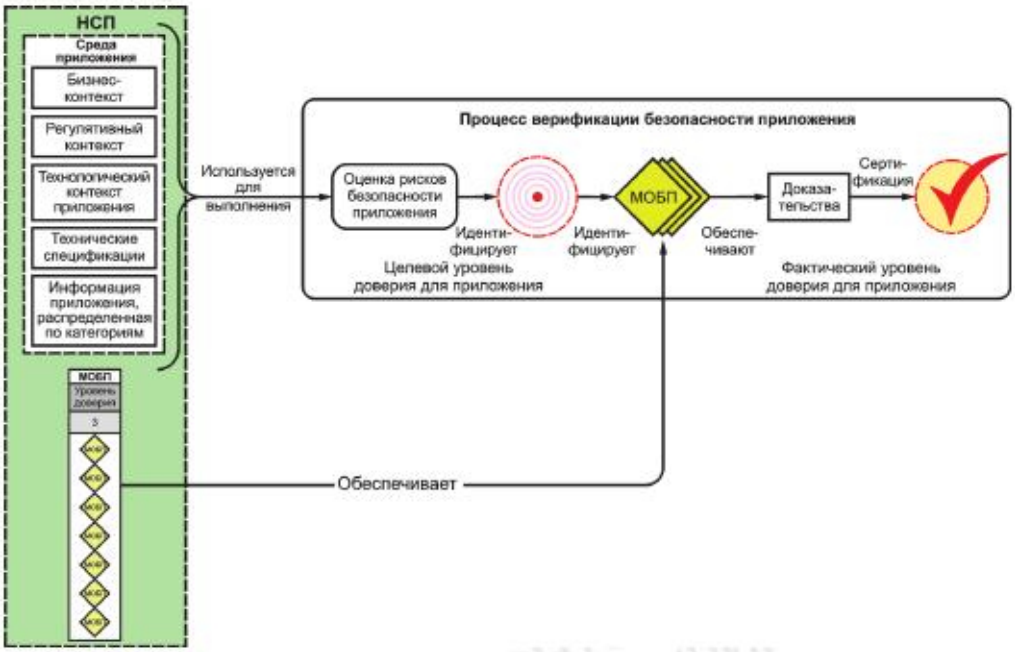

Рисунок 9 — Процесс верификации безопасности приложений

На рисунке 9 показаны ключевые этапы процесса верификации безопасности приложения, которые необходимо выполнить для оценки фактического уровня доверия приложения для приложения. В этот процесс входят следующие мероприятия:

a) определение и подтверждение элементов НСП из НСО;

b) определение и подтверждение рисков безопасности, связанных с приложением;

c) определение и подтверждение требований безопасности приложения, включая минимально необходимые;

d) определение и подтверждение целевого уровня доверия приложения, который соответствует всем определенным требованиям безопасности;

e) подтверждение целевого уровня доверия приложения и получение одобрения владельца приложения;

f) проведение верификационных измерений в отношении МОБП;

g) обновление НСП.

Организация может определить приложение как безопасное, если фактический уровень доверия приложения равен целевому уровню или превосходит его.

Примечание — Данный этап соответствует этапу «Принятие риска информационной безопасности» в рамках процесса менеджмента рисками, приведенного в ИСО/МЭК 27005. Принятие риска осуществляется как до, так и после реализации проекта приложения, на этапах 2 и 5 ПМБП.

7 Элементы нормативной структуры приложения

7.1 Общие положения

7.1.1 Назначение

Нормативная структура приложения (НСП) является официальным источником подробной информации, необходимой конкретному приложению для достижения целевого уровня доверия приложения.

Это истории элементов, решений и результатов, накопленных в течение жизненного цикла приложения.

7.1.2 Описание

Требования безопасности в НСП основаны на оценке рисков, связанных с использованием приложения организацией (этап 2 ПМБП).

НСП создается для каждого проекта приложения и наполняется информацией о технологическом и регулятивном контекстах, а также бизнес-контексте, спецификациях приложений и соответствующих МОБП. Таким образом, НСП является подмножеством или уточнением НСО.

НСП определенного проекта приложения содержит компоненты, представленные ниже. На рисунке 10 приведено графическое представление НСП.

Рисунок 10 — Нормативная структура приложения

НСП существует и может развиваться в течение всего жизненного цикла приложения. Например, регулятивный контекст приложения может измениться, или владелец приложения может предоставить проектной группе приложения новый целевой уровень доверия приложения. В этих случаях организация может добавить новые элементы в НСП или удалить старые.

Изменения в НСП могут повлиять на безопасность приложения. Владелец приложения должен подтвердить эти изменения.

НСП для конкретного проекта приложения содержит различные компоненты, которые приведены в следующих подразделах.

7.2 Компонент: бизнес-контекст приложения

7.2.1 Назначение

Этот компонент используется для хранения бизнес-элементов, определенных, идентифицированных и обработанных в проекте приложения. В этом компоненте представлен утвержденный стандартизированный подход для снижения рисков, связанных с бизнес-контекстом приложения в течение жизненного цикла безопасности. Он описывает варианты с точки зрения бизнеса, применимые к целевому приложению. Бизнес-элементы приложения, определенные на этом этапе, используются для поиска частей НСО при составлении НСП.

7.2.2 Описание

Бизнес-контекст приложения — это задокументированный перечень всех бизнес-процессов, стандартов и лучших практик, связанных с проектом приложения, которые, в основном, берутся из НСО. Реализация и эксплуатация приложения могут быть связаны с рисками. Организация должна оценить риски, определить требования безопасности и МОБП для снижения этих рисков. Специалисты по реализации МОБП должны знать, почему предоставляются данная МОБП, т. е. к какому требованию в области безопасности эти МОБП относятся. Эту необходимую информацию специалисты должны найти в компоненте бизнес-контекста НСП.

7.2.3 Содержание

Бизнес-контекст должен предоставить:

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

b) документы или данные, представляющие сферы деятельности, ограничения и способы ведения дел в организации и ее бизнес-направления: процессы управления приложениями, бизнес-процес-

сы, адаптированные для приложений, включая в себя директивы и внутренние правила бизнес-подразделений;

c) список процессов, политик и лучших методов работы для всех сфер деятельности организации, где будут использовать приложения, например:

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

2) политики безопасности организации, относящиеся к проекту приложения;

3) перечень соответствующих информационных активов организации с различными уровнями безопасности;

4) методология разработки, используемая в проекте приложения;

5) лучшие практики для языков программирования, технического обслуживания, поддержки или непредвиденных ситуаций, используемые в проекте приложения и перечисленные в технологическом контексте;

6) актуальные для проекта приложения стандарты, например стандарты ИСО/МЭК и производственные стандарты, которым организация обязалась соответствовать;

d) список рисков, сопутствующих вышеупомянутыми процессам, политикам и лучшим методами работы и имеющих отношение к безопасности этого приложения;

e) список требований безопасности для снижения вышеуказанных рисков;

f) целевой уровень доверия приложения и фактический уровень доверия приложения;

g) список МОБП, который должен быть реализован и проверен, включая их результаты.

Бизнес-контекст включает в себя описание того, что и как должно выполнять приложение.

7.2.4 Рекомендации

Бизнес-функции в действиях процесса должны быть разработаны и определены как элементарные требования приложению.

В рамках бизнес-функций сценарии управления должны определяться как требования.

7.3 Компонент: регулятивный контекст приложения

7.3.1 Назначение

Этот компонент используется для хранения значимых правовых и нормативных требований, применимых в тех местах, где приложение используется или развернуто. Таким образом, формируется обоснование для некоторых требований безопасности приложения и МОБП.

7.3.2 Описание

Регулятивный контекст приложения включает в себя все законы, нормы и правила, действующие на определенной территории или в рамках определенной юрисдикции, которые влияют на реализацию/эксплуатацию приложения или использование этим приложением данных (например, риски, связанные с разными национальными законами в тех странах, где используется приложение).

7.3.3 Содержание

Регулятивный контекст должен предоставить:

a) список законов и правил, применимых в местах, где приложение используется или развернуто;

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

c) список требований безопасности для снижения вышеуказанных рисков.

7.3.4 Рекомендации

Периодический пересмотр правовых и нормативных мер необходим для обеспечения соответствия отраслевым стандартам и обновленным технологиям для защиты персональных данных потребителя.

Процесс определения того, какие нормативные характеристики применимы к приложению, должен учитывать следующее:

a) пользователей приложения. Например, если дети младше определенного возраста являются целевыми пользователями приложения, к такому приложению могут применяться определенные правила;

b) данные, которые обрабатываются приложением. Например, определенные финансовые данные, такие как сведения о кредитной карте, имеют нормативные спецификации, регулирующие обработку таких данных и управление ими;

c) бизнес-контекст приложения. Например, к компаниям, акции которых торгуются публично, применяются определенные правила в отношении финансовой точности, которые могут повлиять на приложения, обрабатывающие транзакции в организации;

d) географический контекст. Правила, которые распространяются на приложение, зависят от нескольких аспектов его местоположения. Например, это местоположение организации, эксплуатирующей программное обеспечение, а также местоположение целевой аудитории и данные о местоположении. Степень влияния каждого из аспектов зависит от регулятивного контекста.

Можно привести другие примеры:

a) данные — это персональные данные и данные, относящиеся к продуктам, экспорт которых ограничен;

b) персональные данные, регулируемые в некоторых странах законами о конфиденциальности или защите данных;

c) подробное описание регулятивного контекста приложения содержится в ИСО/МЭК 27034-2:2015 (подпункт 5.5.3.4).

7.4 Компонент: технологический контекст приложения

7.4.1 Назначение

Этот компонент помогает определить риски безопасности, исходящие от технологической инфраструктуры приложения. Он предоставляет информацию о том, какие ИТ-компоненты могут использоваться для поддержки МОБП, требующих подобной поддержки.

7.4.2 Описание

Технологический контекст — это документация об ИТ-компонентах приложения (например, физических компонентах, приложениях, услугах, включая их конфигурацию и параметры) и собственных передовых практиках и правилах организации в отношении использования таких компонентов.

7.4.3 Содержание

Технологический контекст должен предоставить:

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

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

c) список требований безопасности для снижения вышеуказанных рисков.

Технологический контекст включает в себя информацию о том, как разрабатывается приложение (например, собственными силами, через аутсорсинг или по смешанной схеме), как оно приобретается (например, это может быть продукт, который размещается на коммерчески готовой ОС (COTS), собственное, приложение с открытым исходным кодом или гибридное приложение) и как развертывается (например, в частном центре обработки данных, в общедоступном облаке, локально на мощностях клиента или в гибридной среде). Технологический контекст должен включать в себя описание оборудования и компонентов приложения (серверы баз данных, серверы приложений и т. д.), языков программирования, инфраструктуры, продуктов с открытым исходным кодом или сторонних продуктов, используемых для приложения. Каждый из этих аспектов будет определять методы, позволяющие приложению достигать согласованного уровня обслуживания, которые должны учитываться при выборе и внедрении МОБП.

7.4.4 Рекомендации

Компонент технологического контекста предоставляет технологическое описание и требования к приложению. В нем указаны доступность, целостность и конфиденциальность данных, используемых приложением. Он определяет соглашение об уровне обслуживания, которое приложение будет обеспечивать для организации.

Соглашение об уровне обслуживания для приложения также определяет технологические методы, используемые для удовлетворения этих требований.

Пример — Кластеризация программного обеспечения на виртуальных серверах с использованием избыточного оборудования, которое обращается к высоконадежному хранилищу со встроенным резервированием для репликации хранилища за пределами площадки в целях обеспечения возможности аварийного восстановления.

Группа НСО поможет определить бизнес-требования в отношении доступности, целостности и конфиденциальности данных, используемых приложением.

Технологический контекст приложения формируется или уточняется с учетом технологического контекста НСО организации и включает в себя все технологические компоненты приложения, такие как архитектура, инфраструктура, протоколы и языки программирования.

Часть технологического контекста среды для приложения определяет технологический стек и (или) инфраструктуру, на которой приложение построено, которую оно использует или с которой взаимодействует. Эта часть спецификации приложений будет использоваться на последующих этапах ПМБП для определения применимых мер обеспечения безопасности приложения из нормативной структуры организации и включения итоговых совпадений в нормативную структуру приложений.

Кроме того, технологический контекст позволяет включать в МОБП конкретные учебные материалы, демонстрирующие рекомендации по разработке и тестированию для каждого требования в технологическом контексте, используемом приложением.

7.5 Компонент: технические спецификации

7.5.1 Назначение

Этот компонент используется для хранения информации, помогающей выявить и снизить риски безопасности, вытекающие из спецификаций приложений, а также риски неправильной реализации и (или) неправильного использования этих спецификаций.

7.5.2 Описание

Компонент спецификаций приложения представляет собой документацию об общих ИТ-требованиях приложения. Он должен содержать все спецификации, функциональные возможности и службы, предоставляемые приложениями или входящими в них, включая в себя документацию и лучшие методы работы для внедрения, использования и проверки.

Спецификации приложения могут иметь форму функциональных, а также нефункциональных требований, а также требований безопасности.

Спецификации безопасности и спецификации, которые влияют на безопасность, особенно важны для ПМБП. Примерами спецификаций безопасности являются минимальные требования безопасности, такие как хранение, передача и настройка паролей, а также средства управления сеансами. Примерами спецификаций, влияющих на безопасность, являются требования к тому, как конечные пользователи и уровни приложений проходят аутентификацию в отношении друг друга.

7.5.3 Содержание

Хранилище спецификаций приложений должно предоставить:

a) список всех спецификаций приложений, включенных в приложение или предлагаемых им;

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

c) перечень рисков, связанных с применением указанных выше спецификаций;

d) список требований безопасности для снижения вышеуказанных рисков.

7.5.4 Рекомендации

Спецификации приложения подробно описывают шаги для выполнения каждой функции приложения. Кроме того, все данные, используемые, хранимые, обрабатываемые, разделяемые и передаваемые приложением, должны быть определены и распределены по категориям. К этим данным относятся все входные и выходные данные, данные конфигурации, данные приложения и данные пользователя.

Информация для построения этого компонента НСП должна быть получена из документированной архитектуры приложения.

По возможности, спецификации приложений должны быть связаны с предварительно одобренными решениями организаций, доступными в компоненте НСО под названием «Хранилище спецификаций приложений». 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 повторного использования таких решений в проектах приложений очевидно.

Подробнее данный компонент рассмотрен в ИСО/МЭК 27034-2:2015 (подпункт 5.5.5.4).

7.6 Компонент: действующие субъекты приложения: роли, обязанности и квалификация

7.6.1 Назначение

Этот компонент помогает определить и снизить риски безопасности, исходящие от людей, работающих с приложениями. Этот компонент также помогает гарантировать, что все критические роли для всех процессов назначены, все обязанности распределены, предотвращены конфликты интересов, а также что сотрудники, назначенные на данные роли, имеют достаточную профессиональную квалификацию.

7.6.2 Описание

Этот компонент представляет собой документацию о ролях, обязанностях и необходимой квалификации для действующих субъектов, связанных с приложением.

7.6.3 Содержание

Список ролей основан на перечне, приведенном в ИСО/МЭК 27034-5:2017 (подраздел 6.6).

a) Любая роль.

Эту роль играют все перечисленные далее действующие субъекты и заинтересованные стороны.

b) Приобретающая сторона.

Лицо, которое приобретает или получает продукт или услугу у поставщика. Действующие субъекты, выступающие в этой роли, являются членами группы по управлению бизнесом.

c) Архитектор приложения.

Лицо, ответственное за определение архитектуры приложения, в том числе ключевые технические решения, которые определяют его общую конструкцию, обеспечение поддержки и реализацию. Действующие субъекты, выступающие в этой роли, являются членами группы разработки.

d) Администратор приложения.

Лицо, ответственное за параметризацию и предоставление доступа к приложению. Действующие субъекты, выступающие в этой роли, являются членами группы по управлению ИТ.

e) Оператор приложения.

Лицо, ответственное за работу приложения и управление им.

Примечание — Оператор приложения может отвечать за управление правами пользователя приложения, функциональность и интерфейсы приложения (например, sysop, sysadmin).

f) Руководство, несущее ответственность.

Самый высокопоставленный персонал, несущий ответственность за безопасное использование приложения в организации. Действующие субъекты, выступающие в этой роли, являются членами группы «Ответственные руководители».

g) Аудитор.

Лицо, которое проводит официальную, систематическую проверку безопасности приложения. Лицо, которое играет эту роль, может быть членом внутренней (проводящей внутренний аудит) или внешней (проводящей внешний аудит) группы экспертов.

h) Директор по (информационной) безопасности (CSO/CISO).

Лицо, ответственное за определение и поддержку мер обеспечения безопасности в организации. Действующие субъекты, выступающие в этой роли, являются членами группы «Ответственные руководители».

i) Разработчик.

Лицо, ответственное за разработку части или всего приложения, в том числе конструирование, прототипирование, реализацию, тестирование элементов и интеграцию компонентов в решение. Действующие субъекты, выступающие в этой роли, являются членами группы разработки.

j) Специалист в предметной области.

Лицо, знакомое с предметной областью, которое может предоставить детальную информацию о предметной области. Действующие субъекты, выступающие в этой роли, являются членами группы внешних экспертов.

k) Администратор ИТ-инфраструктуры.

Лицо, ответственное за параметризацию и предоставление доступа к инфраструктуре приложения. Действующие субъекты, выступающие в этой роли, являются членами группы по управлению ИТ.

l) Архитектор ИТ-инфраструктуры.

Лицо, ответственное за проектирование технологической инфраструктуры, требуемой для предоставления услуг. Действующие субъекты, выступающие в этой роли, являются членами группы по управлению ИТ.

m) Эксперт по ИТ-инфраструктуре.

Лицо ответственное за реализацию и поддержку технологической инфраструктуры. Действующие субъекты, выступающие в этой роли, являются членами группы по управлению. Например, агенты, операторы, вспомогательный персонал, администраторы приложений, системные администраторы, для которых запущено приложение, группы аварийного восстановления и группы обработки и обеспечения безопасности инфраструктуры.

n) Эксперт в области законов и нормативных актов.

Лицо, знакомое с областью законодательства и регламентирующих норм, которое может предоставить детальную информацию о предметной области. Действующие субъекты, выступающие в этой роли, являются членами группы внешних экспертов.

o) Руководитель.

Лицо, ответственное за планирование и управление работой группы лиц, мониторинг их работы и принятие корректирующих мер в случае необходимости. Действующие субъекты, выступающие в этой роли, являются членами группы по управлению бизнесом, т. е. содействуют непрерывности бизнеса.

p) Владелец информации.

Лицо, отвечающее за определение, поддержку и утверждение порядка безопасного использования информации. Действующие субъекты, выступающие в этой роли, являются членами группы по управлению бизнесом.

Примечание — Одна и та же информация может использоваться несколькими приложениями, поэтому важно, чтобы защита информации в различных приложениях утверждалась владельцем информации в дополнение к владельцу приложения.

q) Владелец приложения.

Лицо, отвечающее за определение, поддержку и утверждение порядка безопасного использования приложения. Действующие субъекты, выступающие в этой роли, являются членами группы по управлению бизнесом.

r) Владелец процесса.

Лицо, отвечающее за определение, поддержку и утверждение порядка безопасного использования процесса. Действующие субъекты, выступающие в этой роли, являются членами группы по управлению бизнесом.

s) Менеджер проекта.

Лицо ответственное за планирование и координацию ресурсов, необходимых для достижения целей проекта в рамках запланированной цены, сроков и показателей качества. Действующие субъекты, выступающие в этой роли, являются членами группы по управлению бизнесом.

t) Архитектор безопасности.

Лицо, ответственное за разработку мер обеспечения безопасности в целях снижения уровня угроз безопасности. Действующие субъекты, выступающие в этой роли, являются членами группы разработки.

u) Поставщик.

Юридическое или физическое лицо, заключающее соглашение с приобретающей стороной о поставке продукта или услуги. Действующие субъекты, играющие эту роль, являются членами группы по управлению бизнесом и могут быть поддержаны представителями группы внешних экспертов.

v) Тестировщик.

Лицо, ответственное за внедрение и реализацию тестов в целях обеспечения соответствия развертываемых релизов и сервисов требованиям. Действующие субъекты, играющие эту роль, могут быть членами группы разработки, группы обеспечения качества или группы тестирования информационной безопасности.

w) Преподаватель.

Лицо, которое обучает людей. Физическое лицо, которое играет эту роль, может быть членом внутренней или внешней группы экспертов.

x) Пользователь.

Лицо, выполняющее одну или несколько задач с приложением. Действующие субъекты, выступающие в этой роли, являются членами группы пользователей.

7.6.4 Рекомендации

7.6.4.1 Общие положения

Информация для создания этого компонента должна поступать из бизнес-архитектуры приложения.

Как минимум каждая НСП должна включать в себя владельца приложения. Необходимо определить всех остальных действующих субъектов, взаимодействующих с приложением в течение жизненного цикла. Для каждого действующего субъекта должны быть указаны ожидаемые роли, обязанности и квалификация. Информация о требуемой квалификации должна поступать из компонента НСО «Репозиторий ролей, обязанностей и квалификаций».

Действующий субъект — это лицо или автоматизированный процесс, осуществляющий деятельность в течение жизненного цикла приложения или инициирующий взаимодействие с любым процессом, который выполняется в рамках приложения или на который это приложение влияет.

Дополнительные действующие субъекты могут быть записаны в НСП. Ниже приводится неполный список общих ролей и лиц, которые вовлечены (взаимодействуют напрямую или косвенно) в работу с приложениями:

7.6.4.2 Проектная группа

Проектная группа состоит из лиц, вовлеченных в проект приложения на этапе подготовки к работе или этапе эксплуатации жизненного цикла приложений, таких как архитекторы, аналитики, программисты и тестировщики.

Эти лица также несут ответственность за выбор элементов из НСО для создания или поддержки нормативной структуры приложения для проекта приложения.

7.6.4.3 Группа по эксплуатации

Группа по эксплуатации состоит из лиц, участвующих в управлении и сопровождении приложения на этапе эксплуатации в рамках жизненного цикла приложения, таких как системные администраторы, администраторы баз данных, сетевые администраторы или технические специалисты.

7.7 Компонент: избранные МОБП для этапов жизненного цикла приложения

7.7.1 Назначение

Этот компонент документирует меры обеспечения безопасности, выбранные для приложения, чтобы упростить их утверждение, использование и верификацию, а также обмен данными между ними.

7.7.2 Описание

Меры обеспечения безопасности приложений — это методы, процессы и (или) процедуры, используемые для снижения рисков, появляющихся в организации в результате добавления конкретного приложения.

7.7.3 Содержание

Этот компонент должен предоставить список всех МОБП, выбранных для приложения. Каждая МОБП содержит подробную информацию. Дополнительную информацию см. также в ИСО/МЭК 27034-1 и ИСО/МЭК 27034-5.

7.7.4 Рекомендации

Это приложение должно постоянно контролироваться с целью анализа рисков в течение всего жизненного цикла приложения. Все риски должны быть выявлены и снижены в соответствии с целевым уровнем доверия приложения.

В результате выполнения этапов 1 и 2 ПМБП все МОБП выбираются из библиотеки МОБП организации для конкретного приложения в соответствии со следующими критериями:

a) целевой уровень доверия приложения;

b) требования организации к приложению;

c) конкретные контексты использования приложения и спецификации.

НСП хранит и документирует соответствующие МОБП.

Каждая МОБП предоставляет действия по обеспечению безопасности, которые должны выполняться проектной группой приложения для снижения определенной угрозы безопасности. Оно также предоставляет верификационное измерение, выполняемое группой по верификации, чтобы подтвердить, что соответствующие действия по обеспечению безопасности были успешно выполнены путем изучения соответствующих доказательств. Каждая МОБП также содержит указатели на конкретные этапы в жизненном цикле приложения, где выполняются указанные мероприятие и измерение.

Организация должна определить и одобрить МОБП до начала разработки. Тогда разработчикам не нужно будет создавать их для каждого нового проект приложения. Это гарантирует унифицированный подход организации к выполнению требований по обеспечению безопасности приложения.

Выбранные МОБП должны включать в себя как минимум все МОБП, которые группа НСО утвердила для нулевого уровня доверия приложения, определяемого как минимальный уровень доверия приложения, принимаемый организацией. МОБП, утвержденные для нулевого уровня доверия приложения, не должны изменяться проектной группой в ходе реализации проекта приложения.

7.8 Процессы, связанные с безопасностью приложения

7.8.1 Назначение

Целью этого компонента НСП является помощь проектной группе в определении параметров безопасности приложения, обеспечении управления ими и их верификацию.

7.8.2 Описание

Эти процессы помогают проектной группе интегрировать действия по обеспечению безопасности в знакомые процессы управления жизненным циклом.

7.8.3 Содержание

Этот компонент описывает процессы уровня приложения, такие как:

a) процессы, связанные с безопасностью приложения (подпункт 6.3.6.2);

b) процессы, связанные с НСП (подпункт 6.3.6.3).

7.8.4 Рекомендации

При создании НСП соответствующие процессы должны быть выбраны из НСО и импортированы в НСП. Это дает гарантию, что процессы каждого проекта приложения соответствуют требованиям организации и нормализуются по всей организации.

7.9 Компонент: жизненный цикл приложения

7.9.1 Назначение

Цель этого компонента — помочь проектной группе беспрепятственно интегрировать действия по обеспечению безопасности и верификационные измерения, определенные в МОБП, с действиями, происходящими в течение жизненного цикла приложения, с которым проектная группа уже знакома.

7.9.2 Описание

Жизненный цикл приложения является подмножеством эталонной модели жизненного цикла безопасности приложения [см. ИСО/МЭК 27034-1:2011 (подпункт 8.1.2.7)] в НСО. Жизненный цикл для конкретного проекта будет содержать только процессы, необходимые для проекта приложения. Например, проект, разрабатываемый внутри организации, не будет включать в себя процессы, связанные с аутсорсингом.

7.9.3 Содержание

Этот компонент НСП должен обеспечивать сопоставление жизненного цикла приложения с эталонной моделью жизненного цикла безопасности приложения.

7.9.4 Рекомендации

В организациях разные модели жизненного цикла зачастую используются разными группами разработчиков, в разных подразделениях и в разных проектах.

Поэтому МОБП, которые в НСО ссылаются на действия из стандартизированной эталонной модели жизненного цикла безопасности приложения, должны быть «переданы» до того, как будут сообщены проектным группам, чтобы их можно было интегрировать в привычную модель жизненного цикла каждой группы. НСО содержит этот перевод (также называемый «сопоставлением») для каждой из моделей жизненного цикла организации [см. ИСО/МЭК 27034-2:2015 (пункт 5.5.10)].

Процедура сопоставления, предоставляемая в этом компоненте, используется именно для этой цели. Это могут быть просто таблицы, такие как «Типы перечислений», приведенные в ИСО/МЭК ТС 27034-5-1.

При построении НСП приложения соответствующее отображение затем создается в НСП, сохраняя только этапы жизненного цикла и действия, относящиеся к конкретному проекту приложения.

Как эталонная модель, так и жизненный цикл определенного приложения уже рассматривались в ИСО/МЭК 27034-1:2011 (подпункт 8.1.2.7). Именно в различных процессах в жизненном цикле безопасности приложения, с которыми группа исполнения и группа верификации уже знакомы, выполняются действия и измерения, определенные МОБП. Так формируется ориентированное на процесс представ-

ление о мерах и действиях по обеспечению безопасности приложений и их взаимозависимости. Таким образом, предпочтительным подходом является плавная интеграция МОБП как неотъемлемой части жизненного цикла приложения, а не как действий по обеспечению безопасности, отличных от жизненного цикла.

7.10 Информация, используемая приложением

7.10.1 Назначение

Цель этого компонента НСП состоит в том, чтобы упростить категоризацию безопасности информации/данных приложения и помочь проектной группе отобразить поток критической информации и выполнить оценку рисков безопасности приложения.

7.10.2 Описание

На основе классификации информации/данных приложения для каждой установленной роли определяется управление доступом к данным.

7.10.3 Содержание

Этот компонент предоставляет описание каждой значимой информационной группы приложения (пункт 7.10.4) с метаданными, описывающими категоризацию безопасности информации с точки зрения конфиденциальности, целостности и доступности.

7.10.4 Рекомендации

Понимание информации, которая проходит через приложение, является ключевым шагом для определения требований безопасности. Информация поступает из различных источников. В этом пункте рассматривается вся информация, используемая приложением, в том числе описание контекстов/процессов, код приложения, параметры приложения, пользовательские данные и т. д. Вся эта информация должна быть идентифицирована и классифицирована.

Рисунок 11 — Область безопасности приложений

В ИСО/МЭК 27034-1:2011 (подраздел 6.3) приводится общее определение информации, используемой приложением, эта информация сгруппирована (см. рисунок 11). Это представление не означает, что все элементы, находящиеся в указанной области, являются частью приложения. Скорее, эта схема говорит о том, что все эти элементы должны находиться под защитой, чтобы приложение было безопасным. К информации, подлежащей защите, относится:

a) Информация, определяемая бизнес-контекстом приложения.

Бизнес-контекст относится ко всем связанным с бизнесом лучшим практикам, правилам и ограничениям, вытекающим из сфер деловой активности, в которых приложение реализовано или эксплуатируется.

Бизнес-контекст может включать в себя критическую информацию, которая должна быть защищена (подраздел 7.2).

b) Информация, определяемая регулятивным контекстом приложения.

Информационный репозиторий регулятивного контекста приложения включает в себя только значимую информацию для этого приложения (подраздел 7.3).

1) Наборы законов, директив и правил, которые регламентируют или ограничивают использование приложения:

i) в регионах, где это приложение используется, эксплуатируется, поддерживается, доступно и (или) где его данные будут сохраняться или резервироваться;

ii) действующими субъектами, подключающимися к этому приложению и получающими доступ и (или) сохраняющими информацию из этих регионов.

c) Информация, определяемая процессами жизненного цикла приложения.

Информация, определяемая процессами жизненного цикла приложения, относится к описанию и результатам требуемых или существующих организационных процессов, используемых и выполняемых в течение жизненного цикла приложения и, возможно, подлежащих защите.

Этот информационный репозиторий жизненного цикла приложения содержит такую информацию, как:

1) роли, обязанности и квалификация всех вовлеченных действующих субъектов;

2) процесс, связанный с механизмом и соответствующими услугами, предоставляемыми приложением;

3) обучение заинтересованных сторон;

4) процессы аудита и присвоения квалификаций;

5) процессы реализации (разработка, управление проектом, сопровождение, контроль версий, тестирование и т. д.);

6) операционные процессы (эксплуатация, поддержка и т. д.).

d) Информация, включенная в процессы, связанные с приложением.

Информация, включенная в процессы, связанные с приложением, относится к обязательным или существующим организационным процессам, созданным или подверженным влиянию критических спецификаций приложения и критических данных, которые необходимо защищать.

1) Описание процессов использования и эксплуатации приложения, таких как:

i) процесс проверки;

ii) процесс распространения и установки/обновления приложения;

iii) процессы использования и управления;

iv) процессы обслуживания, ремонта и замены компонентов приложения и т.д.;

v) внештатные ситуации, процессы резервного копирования и восстановления;

vi) процессы распространения и развертывания;

vii) процессы, необходимые для приложения или те, на которые оно оказывает воздействие.

2) Роли, обязанности и квалификации.

3) Обучение заинтересованных сторон.

e) Информация, включенная в технологический контекст приложения.

Информация, включаемая в технологический контекст приложения и относящаяся к продукту и технологическим компонентам, в том числе их конфигурации и связанным процессам, поддерживающим приложение, может подлежать защите.

Как правило, к этой информации относятся данные, которые генерируются конкретным технологическим контекстом, используемым для удовлетворения потребностей бизнеса:

1) терминалы, сети и другие периферийные устройства;

2) операционные системы, элементы конфигурации и услуги;

3) разрешенные каналы связи и порты;

4) коммерческие и другие продукты, например системы управления базами данных (СУБД), используемые приложением и его технологической инфраструктурой;

5) процессы присвоения квалификаций и иные процессы, связанные с технологическим контекстом;

6) компоненты и продукты, используемые приложением, или находящиеся под его воздействием;

7) разрешенные устройства приложения;

8) операционная система, конфигурация и внешние услуги, необходимые для приложения;

9) транспортные и коммуникационные связи, разрешенные к использованию приложением и его технологической инфраструктурой;

10) физические и электрические характеристики среды приложения (например, операционный офис, серверные комнаты, поставщик облачных услуг и т. д.);

11) терминалы приложения (например, смартфон, планшет, ноутбук и т. д.).

f) Информация, включенная в спецификации приложения.

Информация, включенная в спецификации приложения, относится к описанию функциональных пакетов, данным конфигурации и процессам эксплуатации, которые могут подлежать защите, например:

1) спецификации клиентов приложения;
2) спецификация серверного и n-уровня приложения,
3) спецификации аппаратного обеспечения;
4) спецификации безопасности;
5) описания функциональных возможностей приложения;
6) спецификации клиентских терминалов;
7) спецификации системы управления бизнес-процессами.

g) Информация, включенная в роли и разрешения приложения.

Информация, включенная в роли и разрешения приложения, относится к информации об управлении идентификацией и разрешениях, которую, возможно, придется защищать, например:

1) данные по управлению идентификацией;
2) данные идентификации и аутентификации;
3) данные авторизации.

h) Информация, включенная в данные приложения.

Данные приложения относятся к информации приложения, которая может подлежать защите.

Примером таких данных являются идентификаторы сеанса, сгенерированные структурой приложения, чтобы облегчить предоставление сеанса пользователю. Следует учитывать, что эти данные могут быть неочевидны при наблюдении приложения/системы как черного ящика. Также это могут быть журналы, сгенерированные приложением, и данные GPS.

Данные, связанные с приложением, должны классифицироваться в соответствии с моделью классификации, используемой организацией, например: доступность, конфиденциальность, целостность.

1) данные конфигурации приложения;
2) исполняемый код приложения;
3) исходный код приложения;
4) компоненты библиотек и приложений;
5) документацию критически важных компонентов и функциональных особенностей приложения.

i) Информация, включенная в организационные и пользовательские данные приложения.

Организационные и пользовательские данные приложения относятся к информации, поступающей от организаций, которые реализуют или эксплуатируют приложение, включая данные, поступающие от пользователей, которые могут нуждаться в защите, такие как:

1) сертификаты (информация об открытом ключе);
2) секретные ключи;
3) транзакции;
4) журналы событий;
5) конфигурация;
6) данные кредитной карты или финансовые данные;
7) личные данные;
8) различные входные данные в приложении;
9) сертификаты;
10) особо важные данные;
11) персональные данные;
12) данные о пользовательской конфигурации

Приложение А
(справочное)

Рекомендации для этапа процесса менеджмента безопасности приложения: реализация и эксплуатация приложения

А.1 Рекомендации

А.1.1 Общие положения

Данный этап для группы исполнения и группы верификации упрощается, поскольку они получают в НСП только те МОБП, которые необходимы для достижения целевого уровня доверия в рамках конкретного проекта; при этом каждая МОБП содержит подробную информацию для выполнения действий по обеспечению безопасности, а также связанное с ними верификационное измерение на определенной стадии жизненного цикла. Группы не обязательно должны быть информированы о процессах, которые ведут к созданию НСП.

Группа исполнения проекта приложения реализует или выполняет все конкретные действия по обеспечению безопасности, описанные в части «Действия по обеспечению безопасности» (как приведено в 8.1.2.6.5.3 ИСО/МЭК 27034-1:2011) в каждой МОБП, содержащейся в НСП для приложения.

Для менеджеров проектов НСП является эффективным инструментом, поскольку в НСП подробно изложены задачи, ресурсы, требования к квалификации, трудоемкость выполнения одной задачи в человеко-днях и точное указание на этапе жизненного цикла, на котором должна выполняться каждая задача.

Группа по верификации также сможет оценить эффективность НСП, поскольку в ней содержится детальная информация о верификационных измерениях, которые необходимы для получения свидетельства о том, что мероприятия по обеспечению безопасности выполнены правильно и ожидаемые результаты достигнуты. Таким образом, с помощью формальной регистрации свидетельств группа по верификации может до доставки приложения гарантировать, что оно соответствует требованиям безопасности.

Группа по безопасности и техническая группа также найдут концепцию МОБП полезной, потому что МОБП в НСП для конкретного приложения предоставляют список всех требований безопасности, что позволяет заранее планировать необходимые профессиональные ресурсы.

А.1.2 Статический анализ

Проектные группы должны выполнять статический анализ исходного кода. Статический анализ исходного кода обеспечивает масштабируемую возможность проверки безопасности кода и помогает обеспечить соблюдение политик безопасного кодирования. Группа по безопасности и группа верификации несут ответственность за окончательное завершение работы над НСП с привлечением группы верификации. В эту группу также могут входить услуги малого и среднего бизнеса (МСБ) и услуги консалтингового типа во время запуска МОБП, которые должны знать о сильных и слабых сторонах инструментальных средств статического анализа и быть готовы к дополнению этих инструментальных средств другими инструментальными средствами или анализом, выполняемым человеком, в зависимости от ситуации.

А.1.3 Динамический анализ программы

Верификация программы во время ее выполнения необходима для того, чтобы гарантировать, что программное обеспечение функционирует согласно плану. В рамках процесса верификации должны быть определены инструментальные средства для мониторинга поведения приложения при повреждении памяти, проблемах с привилегиями пользователей и других важных случаях, связанных с безопасностью. В ходе процесса динамического анализа программы используются инструментальные средства анализа наряду с другими методами такими, как фаззинг тестирование, применяемое для достижения необходимых уровней покрытия тестами безопасности.

А.1.4 Фаззинг тестирование

Фаззинг тестирование — это специализированная форма динамического анализа, используемая, чтобы вызвать сбой в программе путем преднамеренного ввода в приложение искаженных или случайных данных. Стратегия фаззинг тестирования определяется исходя из предполагаемого характера использования приложения, а также его технических и функциональных спецификаций.

Группе верификации могут потребоваться дополнительные фаззинг тесты или увеличение объема и продолжительности фаззинг тестирования.

А.1.5 Процесс исключения

Если проектная группа приходит к выводу, что некоторые требования безопасности, изложенные в МОБП, не могут быть реализованы, она должна подать запрос об исключении в группу верификации. Группа верификации рассматривает запрос на исключение, и, если общий риск безопасности при невыполнении требований безопасности является приемлемым, исключение может быть согласовано.

А.1.5.1 Процесс исключения

Организация должна определить и внедрить процесс для обработки случаев, когда МОБП не применимы или не реализуемы для конкретного приложения. Исключения должны быть зарегистрированы в НСП и подтверждены группой верификации. Исключения, требующие принятия остаточного риска, должны быть подписаны владельцем

приложения и должны периодически пересматриваться, чтобы определить, можно ли уменьшить остаточный риск, и (или) понять, что остаточный риск остается приемлемым.

А.1.5.2 Процесс управления изменениями

НСП существует в течение жизненного цикла приложения и может со временем меняться. Например, регулятивный контекст приложения может измениться в ходе реализации проекта, что, в свою очередь, может привести к появлению нового целевого уровня доверия приложения. В этих случаях организация может добавить новые элементы к НСП или удалить старые. Изменения НСП влияют на безопасность приложения. Владелец приложения должен подтвердить изменения, которые постоянно отслеживаются.

В течение жизненного цикла приложения и до проектирования каких-либо изменений следует провести анализ МОБП, чтобы убедиться, что целевой уровень доверия приложения находится на максимально требуемом уровне (согласно МОБП).

Пример — Внутреннее приложение с конфиденциальными данными может быть спроектировано и реализовано так, что средства управления паролями будут соответствовать МОБП для внутренних приложений, аналогично, когда приложение становится общедоступным, может потребоваться расширенный набор МОБП (например, использование https для веб-приложений как обязательное требование).

А.1.5.3 Процесс обратной связи

Организация должна определить и внедрить процесс постоянного улучшения НСО посредством обратной связи с новыми знаниями, предложениями по улучшению МОБП и опытом, полученным в ходе разработки и развертывания приложения. Процесс обратной связи должен быть связан с процессом менеджмента НСО. Этот процесс обозначен на рисунке 1 как «Обеспечивает обратную связь для». Этот процесс должен быть связан с процессом сопровождения НСО, обозначенным на рисунке ИСО/МЭК 27034-1:2011 (рисунок 9) как «Обратная связь с предыдущими и текущими проектами приложений».

Ниже приведены примеры обратной связи с НСО.

Примеры

1 Анализ масштаба угроз приложения может быть улучшен путем использования более новых и инновационных инструментальных средств.

2 Новые меры обеспечения безопасности могут быть добавлены к МОБП с целью снижения вероятности атак на определенные функции.

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 27034-1:2011	IDT	ГОСТ Р ИСО/МЭК 27034-1—2014 «Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия»
ISO/IEC 27034-2	IDT	ГОСТ Р ИСО/МЭК 27034-2—2021 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 2. Нормативная структура организации»
ISO/IEC 27034-5	IDT	ГОСТ Р ИСО/МЭК 27034-2—2021 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 5. Структуры данных протоколов и мер обеспечения безопасности приложений»

Примечание — В настоящей таблице использовано следующее условное обозначение степени соответствия стандартов:

- IDT — идентичные стандарты.

Библиография

[1] ISO/IEC/IEEE 12207, Systems and Software Engineering — Software life cycle process

[2] ISO/IEC 15026 (all parts), Systems and software engineering — Systems and software assurance

[3] ISO/IEC/IEEE 15288, Systems and software engineering — Software Life Cycle Processes

[4] ISO/IEC/IEEE 15289, Systems and software engineering — Content of systems and software life cycle process information products (Documentation)

[5] ISO/IEC 21827, Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)

[6] ISO/IEC/IEEE 24765, Systems and software enginesering — Vocabulary

[7] ISO/IEC 26514, Systems and software enginesering — Requirements for designers and developers of user documentation

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

[9] ISO/IEC 27002, Information technology — Security techniques — Code of practice for information security controls

[10] ISO/IEC 27005, Information technology — Security techniques — Information security risk management

[11] ISO/IEC/IEEE 29148, Software and systems engineering — Life cycle processes — Requirements engineering

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

Ключевые слова: мера обеспечения безопасности приложений (МОБП), нормативная структура организации (НСО), нормативная структура приложения (НСП), процесс менеджмента безопасности приложений (ПМБП)

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. 5,30.

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