ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27034-1— 2014

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность приложений

Часть 1

Обзор и общие понятия

ISO/IEC 27034-1:2011
Information technology — Security techniques — Application security — Part 1: Overview and concepts
(IDT)

Издание официальное

Москва
Стандартинформ
2015

gost.e-ecolog.ru

Предисловие

1 ПОДГОТОВЛЕН Федеральным государственным унитарным предприятием «Всероссийский научно-исследовательский институт стандартизации и сертификации в машиностроении» (ФГУП «ВНИИНМАШ»), Обществом с ограниченной ответственностью «Информационно-аналитический вычислительный центр» (ООО «ИАВЦ») и Обществом с ограниченной ответственностью «Научно-производственная фирма «Кристалл» (ООО «НПФ «Кристалл») на основе собственного аутентичного перевода на русский язык международного стандарта, указанного в пункте 4

2 ВНЕСЕН Техническим комитетом по стандартизации ТК 22 «Информационные технологии»

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 11 июня 2014 г. № 564-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27034-1:2011 «Информационная технология. Методы обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия» (ISO/IEC 27034-1:2011 «Information technology — Security techniques — Application security — Part 1: Overview and concepts»).

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

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

5 ВВЕДЕН ВПЕРВЫЕ

*Правила применения настоящего стандарта установлены в ГОСТ Р 1.0—2012 (раздел 8). 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 (*gost.e-ecolog.ru

© Стандартинформ, 2015

Настоящий стандарт не может быть полностью или частично воспроизведен, тиражирован и распространен в качестве официального издания без разрешения Федерального агентства по техническому регулированию и метрологии

Содержание

0.1 Общая информация . . . IV
0.2 Назначение . . . IV
0.3 Целевая аудитория . . . V
0.4 Принципы . . . VII
0.5 Связь с другими международными стандартами . . . VIII
1 Область применения . . . 1
2 Нормативные ссылки . . . 1
3 Термины и определения . . . 2
4 Сокращения . . . 4
5 Структура ИСО/МЭК 27034 . . . 4
6 Введение в безопасность приложений . . . 5
6.1 Общая информация . . . 5
6.2 Безопасность приложений в сравнении с безопасностью программных средств . . . 5
6.3 Сфера действия безопасности приложений . . . 5
6.4 Требования безопасности приложений . . . 7
6.5 Риск . . . 8
6.6 Расходы на безопасность . . . 9
6.7 Целевая среда . . . 9
6.8 Меры и средства контроля и управления и их цели . . . 10
7 Общие процессы ИСО/МЭК 27034 . . . 10
7.1 Компоненты, процессы и структуры . . . 10
7.2 Процесс менеджмента ONF . . . 10
7.3 Процесс менеджмента безопасности приложений . . . 10
8 Общие понятия . . . 13
8.1 Нормативная структура организации . . . 13
8.2 Оценка риска безопасности приложений . . . 29
8.3 Нормативная структура приложений . . . 30
8.4 Подготовка к работе и эксплуатация приложений . . . 32
8.5 Аудит безопасности приложений . . . 35
Приложение А (справочное) Пример сопоставления существующего процесса разработки с ИСО/МЭК 27034 . . . 38
Приложение В (справочное) Сопоставление ASC существующих стандартов . . . 52
Приложение С (справочное) Сопоставление процесса менеджмента риска из ИСО/МЭК 27005 с ASMP . . . 61
Приложение ДА (справочное) Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации . . . 63
Библиография . . . 64

Введение

0.1 Общая информация

Организации должны обеспечивать защиту своей информации и технологических инфраструктур, чтобы сохранять свой бизнес. Традиционно это происходило на уровне ИТ путем защиты периметра и таких компонентов технологических структур, как компьютеры и сети. Но этого оказывалось недостаточно.

Кроме того, организации все больше стремятся обеспечивать свою защиту на уровне корпоративного управления, используя формализованные, протестированные и проверенные системы менеджмента информационной безопасности (СМИБ). Системный подход способствует эффективности СМИБ, как описано в ИСО/МЭК 27001.

Однако в настоящее время организации сталкиваются с постоянно растущей потребностью защиты своей информации на уровне приложений.

Организациям необходимо обеспечивать защиту приложений от уязвимостей, которые могут быть свойственны самому приложению (например, дефекты программных средств), могут появляться в течение жизненного цикла приложений (например, в результате изменений приложения) или возникать в результате использования приложений в не предназначенных для них условиях.

Системный подход к усиленному обеспечению безопасности приложений обеспечивает свидетельства адекватной защиты информации, используемой или хранимой приложениями организации.

Приложения могут быть получены путем внутренней разработки, аутсорсинга или покупки готового стандартного продукта. Приложения могут быть также получены путем комбинации этих подходов, что может привести к иным последствиям в плане безопасности, требующим рассмотрения и управления.

Примерами приложений являются кадровые системы, финансовые системы, системы обработки текстов, системы менеджмента взаимодействия с клиентами, межсетевые экраны, антивирусные системы и системы обнаружения вторжений.

На протяжении своего жизненного цикла безопасное приложение проявляет необходимые характеристики качества программного средства, такие как предсказуемое исполнение и соответствие, а также выполнение требований безопасности с точки зрения разработки, менеджмента, технологической инфраструктуры и аудита. Для создания надежных приложений, которые не увеличивают подверженность риску выше допустимого или приемлемого уровня остаточного риска и поддерживают эффективную СМИБ, требуются процессы и практические приемы усиленной безопасности, а также квалифицированные лица для их выполнения.

Кроме того, безопасное приложение учитывает требования безопасности, вытекающие из типа данных, целевой среды (бизнес-контекст, нормативный и технологический контексты), действующих субъектов и спецификаций[1)] приложений. Должна существовать возможность получения свидетельств, доказывающих, что допустимый или приемлемый уровень остаточного риска достигнут и поддерживается.

0.2 Назначение

Целью ИСО/МЭК 27034 является содействие организациям в планомерной интеграции безопасности на протяжении жизненного цикла приложений посредством:

a) предоставления общих понятий, принципов, структур, компонентов и процессов;

b) обеспечения процессно-ориентированных механизмов для установления требований безопасности, оценки рисков безопасности, присвоения целевого уровня доверия и выбора соответствующих мер и средств контроля и управления безопасностью, а также верификационных мер;

c) предоставления рекомендаций для установления критериев приемки для организаций, осуществляющих аутсорсинг разработки или оперирования приложениями, и для организаций, приобретающих приложения у третьей стороны;

d) обеспечения процессно-ориентированных механизмов для определения, формирования и сбора свидетельств, необходимых для демонстрации того, что их приложения безопасны для использования в определенной среде;

e) поддержки общих концепций, определенных в ИСО/МЭК 27001, и содействия соответствующей реализации информационной безопасности, основанной на менеджменте риска;

[1)] Спецификация — документ, устанавливающий требования [ГОСТ ISO 9000—2011, пункт 3.7.3].

f) предоставления структуры, содействующей реализации мер и средств контроля и управления безопасностью, определенных в ИСО/МЭК 27002 и других стандартах.

ИСО/МЭК 27034:

a) применяется к программным средствам, лежащим в основе приложений, и к факторам, способным влиять на их безопасность, таким как данные, технология, процессы жизненного цикла приложений, процессы поддержки и действующие субъекты;

b) применяется к организациям любого типа и величины (например, к коммерческим предприятиям, государственным учреждениям, некоммерческим организациям), подвергающимся рискам, связанным с приложениями.

ИСО/МЭК 27034 не предоставляет:

a) рекомендации по физической безопасности и безопасности сети;

b) типы измерения или меры и средства контроля и управления;

c) спецификации безопасного кодирования для любого языка программирования.

ИСО/МЭК 27034 не является:

a) стандартом по разработке прикладных программ;

b) стандартом по менеджменту проектов приложений;

c) стандартом, касающимся жизненного цикла развития программных средств.

Указанные в ИСО/МЭК 27034 требования и процессы предназначены не для реализации по отдельности, а скорее для интеграции в существующие процессы организации. Поэтому организации должны сопоставлять свои существующие процессы и структуры с теми, которые предлагает ИСО/МЭК 27034, облегчая, таким образом, осуществление применения ИСО/МЭК 27034.

В приложении А представлен пример того, как существующий процесс разработки программных средств можно сопоставить с некоторыми компонентами и процессами ИСО/МЭК 27034. В общем, организация в рамках любого жизненного цикла развития должна выполнить сопоставление, описанное в приложении А, и добавить любые недостающие компоненты и процессы, которые необходимы для соответствия ИСО/МЭК 27034.

0.3 Целевая аудитория

0.3.1 Общие сведения

ИСО/МЭК 27034 полезен для следующих групп лиц при осуществлении ими своих обозначенных организационных ролей:

a) руководителей;

b) членов групп подготовки к работе и эксплуатации;

c) лиц, отвечающих за приобретение;

d) поставщиков;

e) аудиторов;

f) пользователей.

0.3.2 Руководители

Руководители — это лица, задействованные в менеджменте приложений в течение их полного жизненного цикла. Применяемые этапы жизненного цикла приложений включают этапы подготовки к работе и этапы функционирования. К руководителям относятся:

a) ответственные за информационную безопасность;

b) руководители проектов;

c) администраторы;

d) ответственные за приобретение программных средств;

e) руководители разработки программных средств;

f) владельцы приложений;

g) руководители среднего звена, которые руководят сотрудниками.

В обязанности руководителей входит:

a) обеспечить баланс между стоимостью реализации и поддержанием безопасности приложений по отношению к рискам и представляемой ценностью приложений для организации;

b) проверять рекомендации аудиторских отчетов относительно принятия или отклонения достигаемого и поддерживаемого приложением целевого уровня доверия;

c) обеспечивать уверенность в соблюдении стандартов, законов и предписаний на основе регулятивного контекста приложения (см. 8.1.2.2);

d) осуществлять надзор за реализацией безопасного приложения;

e) санкционировать целевой уровень доверия в соответствии со специфическим контекстом организации;

f) определять, какие меры и средства контроля и управления безопасностью приложений, а также соответствующие верификационные измерения должны реализовываться и тестироваться;

g) сводить к минимуму расходы на верификацию безопасности приложений;

h) документально оформлять процедуры и политики безопасности для приложений;

i) обеспечивать информирование, обучение и надзор за обеспечением безопасности в отношении всех действующих субъектов;

j) вводить надлежащие формы допуска по информационной безопасности, которые требуют применяемые процедуры и политики информационной безопасности;

k) курировать все планы, связанные с системами безопасности во всей структуре организации.

0.3.3 Члены групп подготовки к работе и эксплуатации

Члены групп подготовки к работе и эксплуатации (общеизвестные как группы проекта) — это лица, вовлеченные в проектирование, разработку и поддержку приложений на протяжении всего их жизненного цикла. К ним относятся:

a) разработчики архитектуры;

b) аналитики;

c) программисты;

d) специалисты по тестированию;

e) системные администраторы;

f) администраторы баз данных;

g) сетевые администраторы;

h) технический персонал.

Члены групп подготовки к работе и эксплуатации должны:

a) знать, какие меры и средства контроля и управления должны применяться на каждом этапе жизненного цикла приложений и по какой причине;

b) знать, какие меры и средства контроля и управления должны быть реализованы в самом приложении;

c) сводить к минимуму влияние вводимых мер и средств контроля и управления безопасностью на мероприятия по разработке, тестированию и документальному оформлению в течение жизненного цикла приложений;

d) проверять соответствие введенных мер и средств контроля и управления безопасностью приложений требованиям соответствующих измерений;

e) иметь доступ к инструментальным средствам и лучшим практическим приемам для рациональной разработки, тестирования и документирования;

f) способствовать экспертной оценке;

g) принимать участие в планировании и разработке стратегии приобретения;

h) устанавливать деловые отношения для получения необходимых товаров и услуг (например, в отношении тендера, оценки и заключения договоров);

i) организовывать удаление элементов, оставшихся после завершения работы (например, управление имуществом / удаление).

0.3.4 Лица, отвечающие за приобретение

К лицам, отвечающим за приобретение, относятся все лица, вовлеченные в процесс приобретения продуктов или услуг.

Лица, отвечающие за приобретение, должны:

a) подготавливать запрос предложений, включающий требования к мерам и средствам контроля и управления безопасностью;

b) выбирать поставщиков, соответствующих заданным требованиям;

c) проверять свидетельства применения мер и средств контроля и управления безопасностью услуг на основе аутсорсинга;

d) оценивать продукты, проверяя свидетельства надлежащей реализации мер и средств контроля и управления безопасностью приложений.

0.3.5 Поставщики

К поставщикам относятся лица, вовлеченные в процесс поставки продуктов или услуг.

Поставщики должны:

a) выполнять требования безопасности приложений, представленные в запросах предложений;

b) подбирать соответствующие заявленным требованиям меры и средства контроля и управления безопасностью приложений для предложений с указанием их стоимости;

c) представлять свидетельства надлежащей реализации требуемых мер и средств контроля и управления безопасностью приложений в предлагаемых продуктах или услугах.

0.3.6 Аудиторы

Аудиторы — лица, которые должны:

a) понимать объем и процедуры, вовлеченные в верификационные измерения в отношении соответствующих мер и средств контроля и управления;

b) обеспечивать уверенность в повторяемости результатов аудита;

c) устанавливать список верификационных измерений, создающих свидетельства того, что приложение достигло целевого уровня доверия, требуемого руководством;

d) применять стандартизированные процессы аудита, основанные на использовании свидетельств, поддающихся проверке.

0.3.7 Пользователи

Пользователи — лица, которые должны:

a) быть уверенными в том, что использование или развертывание приложения является безопасным;

b) быть уверенными в том, что приложения последовательно и своевременно создают надежные результаты;

c) быть уверенными в том, что меры и средства контроля и управления безопасностью приложений и соответствующие верификационные измерения установлены и функционируют надлежащим образом.

0.4 Принципы

0.4.1 Безопасность является требованием

Требования безопасности должны быть определены и проанализированы для каждого этапа жизненного цикла приложений, подробно рассмотрены и управляемы на постоянной основе.

Требования безопасности приложений (см. 6.4) должны трактоваться таким же образом, как и требования функциональных возможностей, качества и удобства в эксплуатации (см. ИСО/МЭК 9126, где представлен пример модели качества). Кроме того, должны быть введены связанные с безопасностью требования в отношении соответствия установленным пределам остаточного риска.

Согласно ИСО/МЭК/ИИЭР 29148 требования должны быть необходимыми, обобщенными, точно выраженными, последовательными, полными, лаконичными, осуществимыми, прослеживаемыми и поддающимися проверке. Эти же характеристики относятся к требованиям безопасности. В документации проектов приложений слишком часто встречаются нечеткие требования, такие как «Разработчик должен обнаруживать все значимые риски безопасности для приложения».

0.4.2 Безопасность приложений зависит от контекста

На безопасность приложений влияет определенная целевая среда. Вид и масштаб требований безопасности приложений определяются рисками, которым подвергается приложение. Риски же зависят от вида контекста. Существует три вида контекста:

a) бизнес-контекст: конкретные риски, проистекающие из сферы бизнеса организации (телефонная компания, транспортная компания, государственное учреждение и т. д.);

b) регулятивный контекст: конкретные риски, проистекающие из местоположения бизнеса организации (права на интеллектуальную собственность и лицензирование, ограничения на криптографическую защиту, авторское право, законы и постановления, законы об обеспечении приватности и т. д.);

c) технологический контекст: конкретные риски, проистекающие из технологий, используемых в бизнесе организации [реинжиниринг, безопасность встроенных инструментальных средств, защита исходного кода программы, использование программы, заранее скомпилированной третьей стороной, тестирование безопасности, тестирование на проникновение, граничная проверка, проверка кода программы, среда информационно-коммуникационной технологии (ИКТ), в которой работает приложение, конфигурационные файлы и некомпилированные данные, привилегии операционной системы для инсталляции и/или функционирования, техническое обслуживание, безопасное распространение и т. д.].

Технологический контекст охватывает технические спецификации приложений (функциональные возможности безопасности, безопасные компоненты, онлайновые платежи, надежные контрольные журналы, криптография, управление полномочиями и т. д.).

Организация может утверждать, что приложение безопасно, но это утверждение действительно только для данной конкретной организации в ее особом бизнес-контексте, регулятивном и технологическом контекстах. Если, например, меняется технологическая инфраструктура приложения или приложение используется для таких же целей в другой стране, то этот новый контекст может влиять на требования безопасности и целевой уровень доверия. Текущие меры и средства контроля и управления безопасностью приложений могут уже неадекватно учитывать новые требования безопасности, и приложение может больше не быть безопасным.

0.4.3 Соответствующие инвестиции в обеспечение безопасности приложений

Затраты на применение мер и средств контроля и управления безопасностью приложений и проведение аудиторских измерений должны быть соразмерны целевому уровню доверия (см. 8.1.2.6.4), требуемого владельцем приложения или руководством.

Эти затраты могут считаться инвестицией, поскольку они уменьшают расходы, обязанности владельца приложений и правовые последствия за нарушение безопасности.

0.4.4 Безопасность приложений должна демонстрироваться

Процесс аудита приложений в ИСО/МЭК 27034-1 (см. 8.5) использует поддающиеся проверке свидетельства, обеспечиваемые мерами и средствами контроля и управления безопасностью приложений (см. 8.1.2.6.5).

Приложение не может быть объявлено безопасным, если аудитор не согласен с тем, что подтверждающие свидетельства, генерируемые верификационными измерениями применяемых мер и средств контроля и управления безопасностью приложений, демонстрируют достижение целевого уровня доверия, требуемого руководством.

0.5 Связь с другими международными стандартами

0.5.1 Общие сведения

На рисунке 1 показана взаимосвязь ИСО/МЭК 27034 с другими международными стандартами.



Рисунок 1 — Взаимосвязь ИСО/МЭК 27034 с другими международными стандартами

0.5.2 ИСО/МЭК 27001, Системы менеджмента информационной безопасности. Требования

ИСО/МЭК 27034 способствует реализации рекомендаций ИСО/МЭК 27001 в сфере, ограниченной безопасностью приложений. В частности, используются следующие подходы:

a) систематический подход к менеджменту безопасности;

b) подход процесса «Планирование—Осуществление—Проверка—Действие»;

c) реализация информационной безопасности на основе менеджмента риска.

0.5.3 ИСО/МЭК 27002, Свод норм и правил менеджмента информационной безопасности

ИСО/МЭК 27002 предоставляет практические приемы, которые организация может реализовать в качестве мер и средств контроля и управления безопасностью приложений, как предлагает ИСО/МЭК 27034. Наибольший интерес представляют меры и средства контроля и управления безопасностью из следующих разделов ИСО/МЭК 27002:2005:

a) раздел 10: Менеджмент коммуникаций и работ;

b) раздел 11: Управление доступом;

c) раздел 12: Приобретение, разработка и эксплуатация информационных систем.

0.5.4 ИСО/МЭК 27005, Менеджмент риска информационной безопасности

ИСО/МЭК 27034 способствует реализации предлагаемого ИСО/МЭК 27005 процесса менеджмента риска в сфере, ограниченной безопасностью приложений. В приложении С настоящего стандарта приводится краткое описание процесса менеджмента риска.

0.5.5 ИСО/МЭК 21827, Проектирование безопасности систем. Модель зрелости процесса® (SSE-CMM®)

ИСО/МЭК 21827 предоставляет базовые практические приемы проектирования безопасности, которые организация может реализовать в качестве мер и средств контроля и управления безопасностью приложений, как предполагает ИСО/МЭК 27034. Кроме того, процессы ИСО/МЭК 27034 способствуют достижению некоторых возможностей процессов, определяющих уровни возможностей процессов по ИСО/МЭК 21827.

0.5.6 ИСО/МЭК 15408-3, Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности

ИСО/МЭК 15408-3 предоставляет требования и элементы действий, которые организация может реализовать в качестве мер и средств контроля и управления безопасностью приложений, как предполагает ИСО/МЭК 27034.

0.5.7 ИСО/МЭК ТО 15443-1, Основы доверия к безопасности информационных технологий. Часть 1: Обзор и основы, и ИСО/МЭК ТО 15443-3, Основы доверия к безопасности информационных технологий. Часть 3: Анализ методов обеспечения доверия

ИСО/МЭК 27034 помогает применять и отражать принципы доверия к безопасности из ИСО/МЭК ТО 15443-1 и содействовать сценариям обеспечения доверия из ИСО/МЭК ТО 15443-3.

0.5.8 ИСО/МЭК 15026-2, Разработка программного обеспечения и систем. Гарантирование систем и программного обеспечения. Часть 2: Сценарии обеспечения доверия

Использование процессов и мер и средств контроля и управления безопасностью приложений из ИСО/МЭК 27034 в проектах приложений непосредственно способствует реализации сценариев обеспечения доверия к безопасности приложений. В частности:

a) утверждения и их обоснования обеспечиваются процессом анализа риска безопасности приложений;

b) свидетельства предоставляются встроенными верификационными измерениями мер и средств контроля и управления безопасностью приложений;

c) соответствие ИСО/МЭК 27034 может использоваться в качестве аргумента во многих подобных сценариях обеспечения доверия.

См. также 8.1.2.6.5.1.

0.5.9 ИСО/МЭК 15288, Разработка программного обеспечения и систем. Процессы жизненного цикла систем, и ИСО/МЭК 12207, Разработка программного обеспечения и систем. Процессы жизненного цикла программных средств

ИСО/МЭК 27034 предоставляет дополнительные процессы для организации, а также меры и средства контроля и управления безопасностью приложений, которые организация может включать как дополнительные мероприятия в существующие процессы жизненного цикла проектирования систем и программных средств, предоставляемые ИСО/МЭК 15288 и ИСО/МЭК 12207.

0.5.10 ИСО/МЭК ТО 29193 (в процессе разработки), Принципы и методы инжиниринга безопасных систем

ИСО/МЭК ТО 29193 предоставляет руководства для инжиниринга безопасности систем или продуктов ИКТ, которые организация может реализовать в качестве мер и средств контроля и управления безопасностью приложений, как предлагает ИСО/МЭК 27034.

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность приложений

Часть 1

Обзор и общие понятия

Information technology. Security techniques. Application security. Part 1. Overview and concepts

Дата введения — 2015—06—01

1 Область применения

ИСО/МЭК 27034 предоставляет организациям руководство, содействующее интеграции безопасности в процессы, используемые для менеджмента приложений.

Данная часть ИСО/МЭК 27034 содержит общий обзор безопасности приложений, а также определения, понятия, принципы и процессы, касающиеся обеспечения безопасности приложений.

ИСО/МЭК 27034 применим для приложений, разработанных в рамках организации или приобретенных у третьей стороны, а также в случаях аутсорсинга разработки или эксплуатации приложений.

2 Нормативные ссылки

В настоящем стандарте использованы нормативные ссылки на следующие международные стандарты. Для датированных ссылок используют только указанное издание. Для недатированных ссылок используют самое последнее издание ссылочного документа (с учетом всех его изменений).

ИСО/МЭК 27000:2009[1)] Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Обзор и терминология (ISO/IEC 27000:2009, Information technology — Security techniques — Information security management systems — Overview and vocabulary)

ИСО/МЭК 27001:2005[2)] Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования (ISO/IEC 27001:2005, Information technology — Security techniques — Information security management systems — Requirements)

ИСО/МЭК 27002:2005[3)] Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности (ISO/IEC 27002:2005, Information technology — Security techniques — Code of practice for information security management

---

[1)] Отменен. Действует ИСО/МЭК 27000:2014. Однако для однозначного соблюдения требований настоящего стандарта, выраженных в датированных ссылках, рекомендуется использовать только данный ссылочный стандарт.

[2)] Отменен. Действует ИСО/МЭК 27001:2013. Однако для однозначного соблюдения требований настоящего стандарта, выраженных в датированных ссылках, рекомендуется использовать только данный ссылочный стандарт.

[3)] Отменен. Действует ИСО/МЭК 27002:2013. Однако для однозначного соблюдения требований настоящего стандарта, выраженных в датированных ссылках, рекомендуется использовать только данный ссылочный стандарт.

Издание официальное

ИСО/МЭК 27005:2011 Информационная технология. Методы и средства обеспечения безопасности. Менеджмент риска информационной безопасности (ISO/IEC 27005:2011, Information technology — Security techniques — Information security risk management)

3 Термины и определения

В настоящем стандарте применены термины по ИСО/МЭК 27000, ИСО/МЭК 27001, ИСО/МЭК 27002, ИСО/МЭК 27005, а также следующие термины с соответствующими определениями.

3.1 **действующий субъект** (actor): Лицо или процесс, осуществляющий деятельность во время жизненного цикла приложения или инициирующий взаимодействие с любым процессом, который обеспечивает или затрагивает приложение.

3.2 **фактический уровень доверия** (actual level of trust): Результат процесса аудита, обеспечивающий свидетельства, подтверждающие, что меры и средства контроля и управления безопасностью приложений, требуемые целевым уровнем доверия приложения, надлежащим образом реализованы, проверены и дают ожидаемые результаты.

3.3 **приложение** (application): Решение в области ИТ, включающее прикладное программное средство, прикладные данные и процедуры, предназначенные для содействия пользователям организации в осуществлении определенных задач или обработке конкретных видов задач ИТ посредством автоматизации процесса или функции бизнеса.

Примечание — Процессы бизнеса включают как людей, так и технологии.

3.4 **эталонная модель жизненного цикла безопасности приложений** (application security life cycle reference model): Модель жизненного цикла, используемая в качестве эталона для введения мероприятий по обеспечению безопасности в процессы, связанные с менеджментом приложений, подготовкой к работе и эксплуатацией приложений, менеджментом инфраструктуры и аудитом приложений.

3.5 **нормативная структура приложений; ANF** (application normative framework — ANF): Совокупность нормативных элементов, выбранных из нормативной структуры организации и значимых для конкретного проекта приложения.

3.6 **владелец приложения** (application owner): Организационная роль, отвечающая за менеджмент, использование и обеспечение защиты приложения и его данных.

Примечания

1 Владелец приложения принимает все решения, касающиеся безопасности приложения.

2 Используемый в настоящем стандарте термин «владелец» является синонимом термина «владелец приложения».

3.7 **проект приложения** (application project): Попытка действий с определенными критериями начала и завершения, направленных на создание приложения в соответствии с заданными ресурсами и требованиями.

[ИСО/МЭК 12207:2008, определение 4.29, модифицированное специально для сферы действия приложений]

Примечание — Для целей ИСО/МЭК 27034 критерии начала и завершения таковы, что весь жизненный цикл приложения включен в проект приложения.

3.8 **мера и средство контроля и управления безопасностью приложения; ASC** (application security control — ASC): Структура данных, содержащая четкое перечисление и описание видов деятельности по обеспечению безопасности и их соответствующего верификационного измерения, подлежащего выполнению в конкретный момент жизненного цикла приложения.

3.9 **процесс менеджмента безопасности приложений; ASMP** (application security management process — ASMP): Используемый организацией общий процесс менеджмента в отношении видов деятельности по обеспечению безопасности, действующих субъектов, артефактов и аудита каждого приложения.

3.10 **прикладное программное средство** (application software): Программное средство, предназначенное для содействия пользователям в осуществлении определенных задач или обработке конкретных видов задач, в отличие от программного средства, управляющего компьютером.

[ИСО/МЭК/ИИЭР 24765:2010, определение 3.130-1]

3.11 **аудит** (audit): Систематический, независимый и документированный процесс получения свидетельств аудита и объективного их оценивания с целью установления степени выполнении согласованных критериев аудита.

[ИСО 9000:2005, определение 3.9.1, обобщенно модифицированное]

3.12 **среда** (environment): Бизнес-контекст, регулятивный и технологический контексты, в которых используется приложение, включая все процессы, продукты, информацию и действующих субъектов, задействованных в приложении.

3.13 **жизненный цикл** (life cycle): Развитие системы, продукта, услуги, проекта или других изготовленных человеком объектов, начиная со стадии разработки концепции и заканчивая прекращением применения.

[ИСО/МЭК 12207:2008, определение 4.16]

3.14 **модель жизненного цикла** (life cycle model): Структура процессов и действий, связанных с жизненным циклом, организуемых на стадиях, которые также служат в качестве общей ссылки для установления связей и взаимопонимания сторон.

[ИСО/МЭК 12207:2008, определение 4.17]

3.15 **сопровождение** (maintenance): Любое изменение приложения, осуществленное после его выпуска.

Пример — Исправление ошибок, добавление функциональных возможностей, улучшение функционирования, обеспечивающие уверенность в функциональности приложения.

3.16 **нормативная структура организации; ONF** (organization normative framework — ONF): Внутренняя структура всей организации, включающая совокупность нормативных процессов и элементов безопасности приложений.

3.17 **группа нормативной структуры организации; группа ONF** (ONF Committee): Организационная роль в нормативной структуре организации, отвечающая за сопровождение и санкционирование компонентов, связанных с безопасностью приложений.

3.18 **операционная среда** (operating environment): Внешнее окружение программы, которое существует или предполагается во время ее выполнения.

[ИСО/МЭК 2382-7:2000, определение 07.11.07]

3.19 **продукция** (product): Результат процесса.

[ИСО 9000:2005, определение 3.4.2]

3.20 **безопасное приложение** (secure application): Приложение, фактический уровень доверия которого равен целевому уровню доверия, который определяется организацией, использующей приложение.

3.21 **целевой уровень доверия** (targeted level of trust): Обозначение или метка совокупности мер и средств контроля и управления безопасностью приложений, сочтенных необходимыми владельцем приложения для снижения связанного с конкретным приложением риска до допустимого (или приемлемого) уровня после анализа риска безопасности приложения.

3.22 **пользователь** (user): Лицо, использующее или эксплуатирующее что-то.

[Краткий оксфордский словарь английского языка]

Примечание — Для целей настоящего стандарта термин «пользователь» обозначает не только конечного пользователя, но также операционные роли и роли сопровождения, такие как системный администратор и администратор баз данных.

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

Примечания

1 Термин «валидирован» используется для обозначения соответствующего статуса.

2 Условия применения могут быть реальными или смоделированными.

[ИСО 9000:2005, определение 3.8.5]

3 На языке неспециалиста «валидация» означает «Правильно ли построено приложение?»

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

Примечания

1 Термин «верифицирован» используют для обозначения соответствующего статуса.

2 Деятельность по подтверждению требований может включать в себя: осуществление альтернативных расчетов, сравнение спецификации на новый проект с аналогичной документацией на апробированный проект, проведение испытаний и демонстраций и анализ документов до их выпуска.

[ИСО 9000:2005, определение 3.8.4]

3 На языке неспециалиста «верификация» означает «Корректно ли построено приложение?»

4 Сокращения

В настоящем стандарте применены следующие сокращения:

ANF — application normative (нормативная структура приложений);

ASC — application security control (мера и средство контроля и управления безопасностью приложений);

ASMP — application security management process (процесс менеджмента безопасности приложений);

COTS — commercial-off-the-shelf (готовый к использованию коммерческий продукт);

ONF — organization normative framework (нормативная структура организации);

XML — extended markup language (расширяемый язык разметки);

ИКТ — информационно-коммуникационная технология (Information and Communication Technology — ICT);

СМИБ — система менеджмента информационной безопасности (Information Security Management System — ISMS).

5 Структура ИСО/МЭК 27034

ИСО/МЭК 27034 состоит из шести частей. В части 1 представлены обзор и общие понятия. Данной части вполне достаточно для оценивания необходимости реализации ИСО/МЭК 27034 в организации, а также для презентации и обучения. Для самой же реализации ИСО/МЭК 27034 данной части недостаточно.

Организациям, желающим применять ИСО/МЭК 27034, необходимы части 2, 3 и 4. Они содержат подробные описания всех представленных в данной части ИСО/МЭК 27034 понятий.

ИСО/МЭК 27034-5 будет особенно полезен организациям, заинтересованным в приобретении или распространении мер и средств контроля и управления безопасностью приложений, так как он предоставляет стандартную структуру данных и стандартный протокол для распространения мер и средств контроля и управления. Например, крупная организация может быть заинтересована в автоматическом распространении и обновлении мер и средств контроля и управления для всех своих подразделений.

ИСО/МЭК 27034-6 содержит примеры мер и средств контроля и управления для конкретных требований безопасности приложений, эта часть будет полезна организациям, желающим реализовать ИСО/МЭК 27034, или организациям, которые хотят разработать определенные меры и средства контроля и управления безопасностью приложений.

Содержание шести частей ИСО/МЭК 27034:

Часть 1 — Обзор и общие понятия

В части 1 представлен обзор безопасности приложений. Она знакомит с определениями, общими понятиями, принципами и процессами, касающимися обеспечения безопасности приложений.

Часть 2 — Нормативная структура организации

В части 2 представлено подробное описание нормативной структуры организации, ее компонентов и процессов менеджмента на уровне организации. В данной части объясняются взаимосвязи этих процессов, связанные с ними мероприятия и способы поддержания ими процесса менеджмента безопасности приложений. В данной части описывается, как организация должна реализовывать ИСО/МЭК 27034 и интегрировать его со своими существующими процессами.

Часть 3 — Процесс менеджмента безопасности приложений

В части 3 представлено подробное описание процессов, вовлеченных в проект приложения: определение требований и среды приложения, оценка риска безопасности приложения, создание и поддержка нормативной структуры приложения, реализация и введение в действие приложения и валидация его безопасности на протяжении всего жизненного цикла. В данной части объясняются взаимосвязи этих процессов, их функционирование и взаимозависимости, а также введение ими безопасности в проект приложения.

Часть 4 — Валидация безопасности приложений

В части 4 представлено углубленное описание процесса валидации безопасности приложений и процесса сертификации, измеряющего фактический уровень доверия приложения и сравнивающего его с целевым уровнем доверия, который заранее выбирается организацией.

Часть 5 — Структура данных управления безопасностью протоколов и приложений

В части 5 представлены протоколы и XML-схема для мер и средств контроля и управления безопасностью приложений (ASC) на основе ИСО/МЭК ТУ 15000 «Расширяемый язык разметки для электронного бизнеса (ebXML)». Данная часть может быть использована для содействия организациям в валидации структуры данных ASC и других компонентов ИСО/МЭК 27034, а также для поддержки распространения, обновления и использования ASC.

Часть 6 — Руководство по безопасности для конкретных приложений

В части 6 представлены примеры ASC, приспособленных к конкретным требованиям безопасности приложений.

6 Введение в безопасность приложений

6.1 Общая информация

Обеспечение безопасности приложений — это процесс применения мер и средств контроля и управления и измерений к приложениям организации с целью осуществления менеджмента риска, возникающего в результате их использования.

Меры и средства контроля и управления и измерения могут применяться к самому приложению (его процессам, компонентам, программным средствам и результатам), его данным (конфигурационным данным, данным пользователей, данным организации) и ко всей технологии, процессам и действующим субъектам, вовлеченным в жизненный цикл приложения.

6.2 Безопасность приложений в сравнении с безопасностью программных средств

Приложение — это решение в области ИТ, включающее программное средство (см. 3.3). Таким образом, безопасность приложений является более широким понятием, охватывающим безопасность программных средств.

6.3 Сфера действия безопасности приложений

6.3.1 Общие сведения

Безопасность приложений обеспечивает защиту критических данных, вычисляемых, используемых, хранимых и передаваемых приложением, как требуется организации. Эта защита обеспечивает уверенность не только в доступности, целостности и конфиденциальности данных, но также в неотказуемости и аутентификации пользователей, имеющих к ним доступ. Критичность данных и иных активов должна определяться организацией посредством процесса оценки риска безопасности.

Нуждающиеся в защите критические данные также могут представлять собой исходный код приложения, двоичный код и исполняемый код.

На рисунке 2 показано графическое представление сферы действия безопасности приложений в виде области, ограниченной пунктирными линиями.

Это представление не означает, что все элементы в показанной выше сфере действия являются частью приложения, а говорит о том, что все эти элементы требуют защиты для обеспечения безопасности приложения. Таким образом, сфера действия безопасности приложения является более широкой, чем сфера действия самого приложения. Приведенная ниже таблица иллюстрирует это отличие.

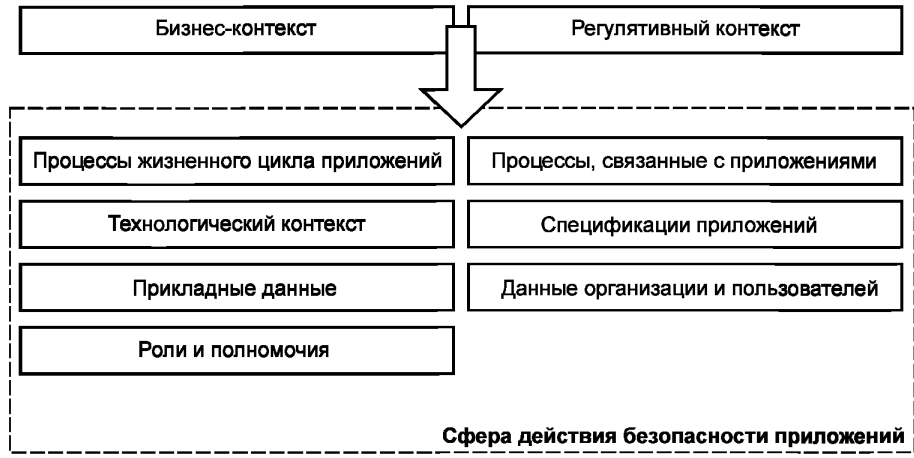

Рисунок 2 — Сфера действия безопасности приложений

Таблица 1 — Сфера действия приложений в сравнении со сферой действия безопасности приложений

Элементы	В сфере действия приложений	В сфере действия безопасности приложений
Данные организации и пользователей (6.3.9)		•
Прикладные данные (6.3.8)	•	•
Роли и полномочия (6.3.10)	•	•
Спецификации приложений (6.3.7)	•	•
Технологический контекст (6.3.6)		•
Процессы, связанные с приложениями (6.3.5)		•
Процессы жизненного цикла приложений (6.3.4)		•
Бизнес-контекст (6.3.2)		•
Регулятивный контекст (6.3.3)		•

Приведенные ниже данные и процессы находятся в сфере действия безопасности приложений и должны быть защищены.

6.3.2 Бизнес-контекст

К бизнес-контексту относятся все связанные с бизнесом лучшие практические приемы, предписания и ограничения, вытекающие из сферы бизнеса организации.

6.3.3 Регулятивный контекст

К регулятивному контексту относятся все законы, предписания и общие правила, вытекающие из места ведения бизнеса или юрисдикции, которые влияют на функциональные возможности приложения или использование его данных (например, риски в результате различия национальных законов в странах, где будет использоваться одно и то же приложение).

6.3.4 Процессы жизненного цикла приложений

Должна обеспечиваться защита всех необходимых или существующих процессов организации, вовлеченных в жизненный цикл приложений, таких как:

a) процессы обучения, аудита и аттестации;

b) процессы реализации (разработка, менеджмент проектов, сопровождение, контроль версий, тестирование и т. д.);

c) операционные процессы.

6.3.5 Процессы, связанные с приложениями

Должна обеспечиваться защита всех необходимых или существующих процессов организации, затрагиваемых важными спецификациями и критическими данными приложений, таких как:

a) процессы использования и менеджмента;

b) процессы сопровождения и резервного копирования;

c) процессы распространения и развертывания;

d) процессы, на которые влияют приложения или которые требуются приложениям.

6.3.6 Технологический контекст

Должна обеспечиваться защита всех продуктов и технологических компонентов, поддерживающих важные спецификации или критические данные, таких как:

a) терминалы, сети и иные разрешенные периферийные устройства;

b) операционная система, конфигурация и сервисы;

c) разрешенные каналы связи и порты;

d) COTS и иные продукты, такие как системы управления базами данных (СУБД), используемые приложениями, и их технологическая инфраструктура;

e) модификация и иные процессы, связанные с технологическим контекстом;

f) продукты, на которые оказывают влияние приложения или которые используются приложениями.

6.3.7 Спецификации приложений

Должна обеспечиваться защита от несанкционированной модификации всех спецификаций приложений, таких как:

a) спецификации аппаратных средств;

b) спецификации безопасности;

c) функциональные возможности приложений;

d) спецификации терминала клиента;

e) спецификации операционного отдела.

6.3.8 Прикладные данные

Должна обеспечиваться защита всей критической информации приложений, такой как:

a) конфигурационные данные приложений;

b) двоичный код приложений;

c) исходный код приложений;

d) компоненты приложений и библиотек;

e) документация важнейших компонентов и функциональных возможностей приложений.

6.3.9 Данные организации и пользователей

Должна обеспечиваться защита всей критической информации, касающейся организации и пользователей, такой как:

a) сертификаты;

b) секретные ключи;

c) необходимые для целевой задачи данные;

d) персональные данные;

e) пользовательские данные конфигурации.

6.3.10 Роли и полномочия

Должна быть обеспечена защита всей критической информации по управлению идентификацией и полномочиями, такой как:

a) данные по управлению идентификацией;

b) идентификационные и аутентификационные данные;

c) данные авторизации.

6.4 Требования безопасности приложений

6.4.1 Источники требований безопасности приложений

Согласно ИСО/МЭК 27005, требования безопасности приложений идентифицируются посредством оценки риска и обработки риска и диктуются такими факторами, как спецификации приложений, целевая среда приложений (бизнес-контекст, регулятивный и технологический контексты), критические данные и выбор, который делает владелец приложений.

Функциональные требования безопасности диктуют, какие функциональные возможности безопасности будут реализованы в приложении. Нефункциональные требования безопасности направлены

на качество безопасности, которое должно проявлять приложение. Все эти меры и средства контроля и управления должны быть полностью определены и утверждены организацией.

6.4.2 Разработка требований безопасности приложений

Разработка требований приложений — это процесс, охватывающий сбор, анализ и определение требований для приложений. Он должен быть дополнен оценкой риска с целью включения требований безопасности.

Как и в случае любых требований, оценка риска должна включать постоянное и систематическое использование процедур, обеспечивающих уверенность в том, что полученная совокупность требований является полной, последовательной, легко понимаемой и анализируемой владельцем приложений. Требования и их выполнение также должны быть измеримыми.

6.4.3 Система менеджмента информационной безопасности

6.4.3.1 СМИБ организации

Вся информация, которую поддерживает и обрабатывает организация, подвергается риску ошибок, хищения, пожара, затопления и т. д., а также опасностям, связанным с используемой технологией. Термин «информационная безопасность» основывается на информации как на активе, имеющем присвоенное значение и требующем соответствующей защиты. Согласно ИСО/МЭК 27000, СМИБ представляет модель для создания, внедрения, функционирования, мониторинга, анализа, поддержки и улучшения защиты информационных активов организации на основе подхода к рискам бизнеса. Защита информационных активов организации должна быть ориентирована на связанные с ними риски и принятые бизнесом уровни риска.

Этот менеджмент рисков основывается на информационной безопасности и охватывает все виды рисков, связанных со всеми видами информации, используемой организацией.

6.4.3.2 Безопасность приложений в контексте СМИБ

Безопасность приложений поддерживает цели СМИБ в масштабах организации, обеспечивая модель создания, реализации, эксплуатации, мониторинга, проверки, поддержки и совершенствования защиты информационных активов организации, связанных с приложениями. Безопасность приложений должна обеспечивать адекватные меры и средства контроля и управления, а также свидетельства, подтверждающие руководителям организации осуществление адекватного менеджмента рисков, связанных с использованием приложений.

СМИБ обуславливает безопасность приложений, обеспечивая уверенность в осуществлении менеджмента всех рисков, связанных с информацией организации, включая информацию, которая доступна приложениям. Меры и средства контроля и управления, назначаемые СМИБ, распространяются на уровень приложений.

6.5 Риск

6.5.1 Риск безопасности приложений

Риск безопасности приложений — это риск, которому подвергаются организации при использовании конкретного приложения.

Риск безопасности приложений возникает при наличии:

a) угроз, направленных на информацию, которая доступна приложениям;

b) уязвимостей;

c) влияния успешного использования уязвимостей угрозами.

Деятельность по идентификации, отслеживанию, хранению информации, измерению и сообщению о рисках приложений крайне важна. Требования безопасности приложений и предназначенные для них меры и средства контроля и управления являются реакцией на этот риск. Процесс оценки риска безопасности приложений является необходимым, потому что риск меняется с течением времени, приводя к необходимости постоянной и последовательной идентификации и хранения информации о риске.

6.5.2 Уязвимости приложений

Уязвимости являются результатом наличия неадекватных мер и средств контроля и управления или их отсутствия. Неадекватно контролируемые уязвимости в результате приводят к неприемлемому риску приложений.

Уязвимости проистекают от:

a) действующих субъектов, таких как программисты, создающие плохие программы, пользователи, делающие ошибки при использовании программного обеспечения, технические специалисты и разработчики, делающие ошибки в процессе поддержки приложения;

b) процессов, таких как неадекватные процедуры тестирования, плохой менеджмент проектов, недостаточное внимание к безопасности в течение процессов жизненного цикла, непредвиденное взаимодействие между приложениями, пользователями и операторами, неадекватные процессы менеджмента изменений;

c) технологического контекста, такого как плохо выбранная технологическая инфраструктура или продукты;

d) особенностей, таких как неадекватное проектирование, уязвимости, обусловленные взаимодействиями в системе или ошибками в интерфейсах компонентов.

6.5.3 Угрозы приложениям

Угроза несет в себе возможность причинения ущерба критической информации в сфере действия приложения и соответственно самой организации. Угрозы проистекают из:

a) среды приложений: регулятивного контекста, бизнес-контекста и технологического контекста;

b) действующих субъектов.

6.5.4 Влияние приложений

Влияние определяется расходами, понесенными организацией в результате нарушения доступности, целостности или конфиденциальности критических данных приложений.

6.5.5 Менеджмент риска

Менеджмент риска приложений — это процесс поддержания рисков безопасности приложений на допустимых уровнях. Это достигается путем обработки рисков безопасности приложений, сочтенных неприемлемыми, посредством применения к ним мер и средств контроля и управления.

Менеджмент риска представляет собой ключевую концепцию в информационной безопасности. Согласно ИСО/МЭК 27005, *«процесс менеджмента риска информационной безопасности может применяться к организации в целом, любой отдельной части организации (например, отделу, физической площадке, услуге), любой информационной системе, существующим, планируемым или конкретным аспектам мер и средств контроля и управления (например, планированию непрерывности бизнеса)».*

Представленный в ИСО/МЭК 27005 процесс менеджмента риска информационной безопасности состоит из установления контекста, оценки риска, обработки риска, принятия риска, коммуникации риска, мониторинга и пересмотра риска.

Процесс менеджмента риска безопасности приложений должен использовать такие же элементы с более точной детализацией и сферой действия, установленной для уровня приложений.

6.6 Расходы на безопасность

Расходы организации на реализацию, поддержку и проверку мер и средств контроля и управления безопасностью должны минимизироваться до допустимого (или приемлемого) уровня после надлежащего рассмотрения рисков и соответствующего влияния использования приложений. Расходы на безопасность должны учитывать потенциальное влияние угроз и уязвимостей.

6.7 Целевая среда

Целевая среда состоит из бизнес-контекста, регулятивного и технологического контекстов, в которых организация будет использовать приложение. Все угрозы, которые могут причинить ущерб приложению, проистекают из этой среды. По этой причине в начале проекта приложения следует четко определить целевую среду приложения.

Для успешного и безопасного использования приложения необходимо соответствие технологического контекста организации требованиям целевой среды приложения. Когда приложение реализуется, технологический контекст организации может потребовать новых продуктов и аппаратных средств, которые могут влиять на безопасность других приложений и риски безопасности организации.

Поскольку риски организации, использующей приложения, проистекают из целевой среды приложения, то должны быть определены новые требования безопасности приложений для учета этих новых рисков и выбора мер и средств контроля и управления, уменьшающих эти риски до допустимого (или приемлемого) уровня. Эти меры и средства контроля и управления безопасностью могут быть введены в процессы жизненного цикла приложений (например, в процесс приобретения или в процесс снятия с эксплуатации), добавлены к исходному коду приложения или интегрированы куда-либо еще в жизненном цикле приложения (см. 8.3.4), когда это будет необходимо организации.

6.8 Меры и средства контроля и управления и их цели

В соответствии с ИСО/МЭК 27001 для выполнения требований, определенных процессами оценки и обработки риска, должны быть выбраны и реализованы меры и средства контроля и управления и их цели. В сфере безопасности приложений процесс оценки риска устанавливает цели мер и средств контроля и управления согласно требованиям безопасности приложений.

7 Общие процессы ИСО/МЭК 27034

7.1 Компоненты, процессы и структуры

ИСО/МЭК 27034 предоставляет компоненты, процессы и структуры, необходимые организациям в приобретении, реализации и использовании надежных приложений с допустимыми (или приемлемыми) расходами на безопасность. Более того, эти компоненты, процессы и структуры обеспечивают поддающиеся проверке свидетельства того, что приложения достигли и поддерживают целевой уровень доверия.

Все компоненты, процессы и структуры являются частью двух общих процессов, взаимосвязь которых показана на рисунке 3:

a) процесса менеджмента ONF;

b) процесса менеджмента безопасности приложений (ASMP).

Эти два процесса используются в организации на разных уровнях и в различных временны́х рамках и имеют разные сферы действия. Процесс менеджмента ONF представляет собой постоянный процесс на уровне организации, а ASMP используется для осуществления менеджмента безопасности конкретных проектов приложений.

7.2 Процесс менеджмента ONF

Процесс менеджмента ONF должен использоваться для менеджмента **связанных с безопасностью приложений** аспектов ONF (см. 8.1). ONF включает все процессы, вовлеченные в безопасность приложений, а также предписания, законы, лучшие практические приемы, роли и обязанности, принятые организацией. Она определяет все виды контекста организации и является уникальной ссылкой для безопасности приложений в организации.

Примечание 1 — Организация обычно использует свою нормативную структуру для других целей, выходящих за пределы области применения ИСО/МЭК 27034, у нее обычно есть определенные процессы для осуществления менеджмента. Таким образом, ONF и процесс ее менеджмента, созданные для целей ИСО/МЭК 27034, являются подмножеством существующей ONF и связанных с ней процессов.

Процессы, связанные с безопасностью приложений, должны быть частью ONF.

Надзор и ответственность за поддержку и утверждение связанных с безопасностью приложений компонентов ONF должны осуществляться организационной ролью, называемой в ИСО/МЭК 27034 «группой ONF».

Примечание 2 — Процесс менеджмента ONF и его компоненты и подпроцессы более детально представлены в 8.1.3.2, а также в ИСО/МЭК 27034-2.

7.3 Процесс менеджмента безопасности приложений

7.3.1 Общие сведения

Процесс менеджмента безопасности приложений — суммарный процесс осуществления менеджмента безопасности для каждого используемого организацией приложения. В приложении С показано, что ASMP представляет собой конкретизацию представленного в ИСО/МЭК 27005 процесса менеджмента риска.

Процесс менеджмента безопасности приложений включает пять шагов:

a) определение требований и среды приложений;

b) оценка рисков безопасности приложений;

c) создание и поддержка нормативной структуры приложений;

d) подготовка к работе и эксплуатация приложений;

e) аудит безопасности приложений.

Примечание — ASMP более детально представлен в разделе 8, а также в ИСО/МЭК 27034-3.

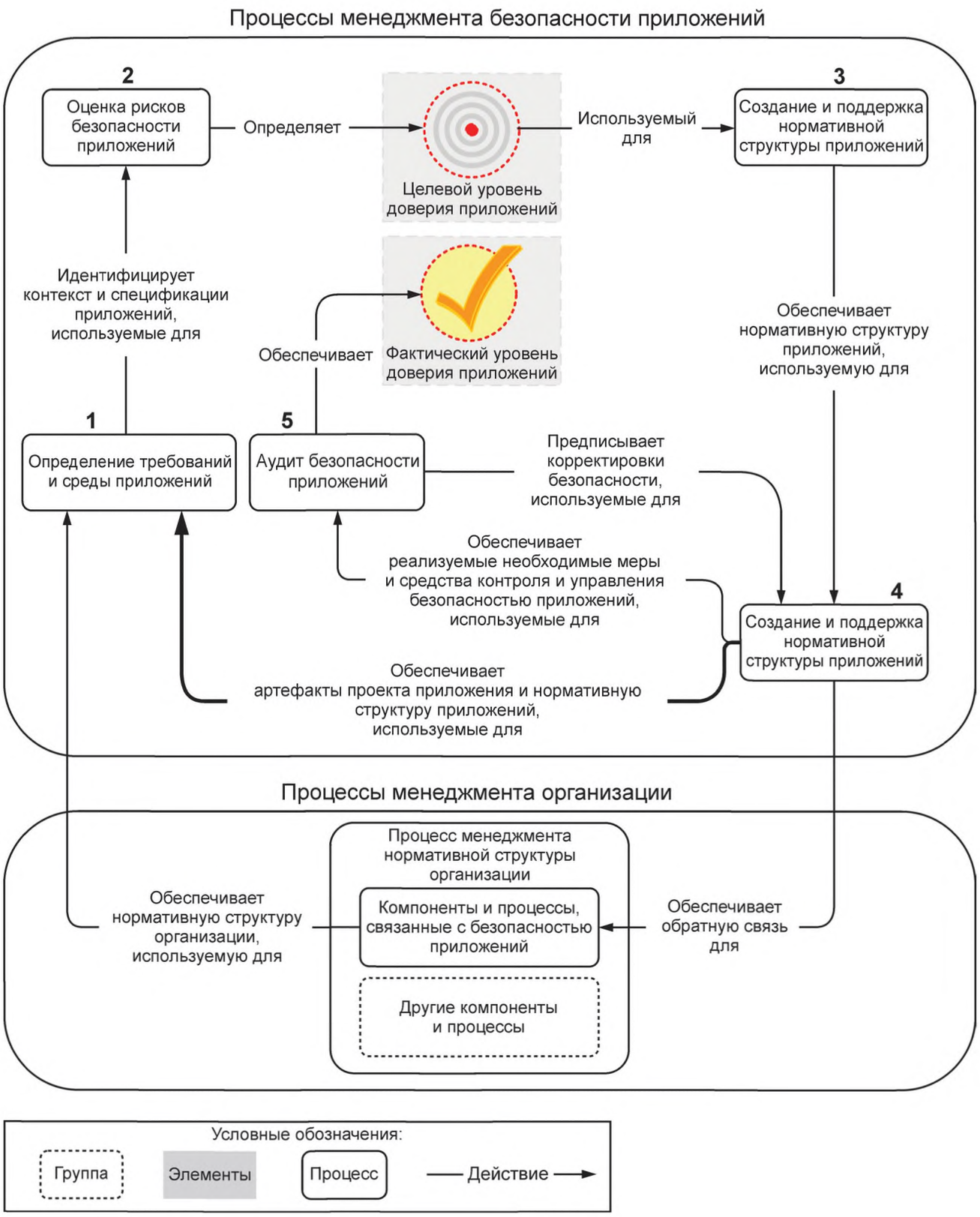

Рисунок 3 — Процессы менеджмента

7.3.2 Определение требований и среды приложений

Первым шагом ASMP является определение всех требований приложений, включая:

a) действующих субъектов;

b) спецификации;

c) информацию;

d) среду.

Среда приложений состоит из:

a) технологического контекста;

b) бизнес-контекста;

c) регулятивного контекста.

Примечание — Контекст более детально представлен в 8.1.2.1—8.1.2.2.

Этот шаг соответствует шагу «определение контекста» в устанавливаемом ИСО/МЭК 27005 процессе менеджмента риска. Он предоставляет необходимую информацию для последующего шага оценки риска.

7.3.3 Оценка рисков безопасности приложений

Второй шаг ASMP представляет собой процесс, соответствующий шагу «оценка риска» и частично шагу «обработка риска» в устанавливаемом ИСО/МЭК 27005 процессе менеджмента риска, с более точным уровнем детальности и сферой действия, ограниченной одним проектом приложения.

Оценка риска состоит из идентификации риска, анализа риска и оценивания риска.

На этом шаге ASMP также создаются требования безопасности, которые используются для получения желаемого уровня доверия для приложения. Он называется целевым уровнем доверия приложения (см. 8.2.4) и должен быть утвержден владельцем приложения.

Данный шаг также соответствует «выбору вариантов обработки риска», относящемуся к шагу «обработка риска» в устанавливаемом ИСО/МЭК 27005 процессе менеджмента риска.

7.3.4 Создание и поддержка нормативной структуры приложений

На третьем шаге ASMP из ONF выбираются все необходимые элементы, применимые к конкретному проекту приложения. Результатом является нормативная структура приложений (ANF). Точное содержание ANF определяет целевой уровень доверия приложений, контекст приложений (регулятивный, технологический и бизнес-контекст), обязанности и профессиональную квалификацию действующих субъектов, а также спецификации приложений.

Именно на этом шаге для проекта приложения организация устанавливает жизненный цикл, который включает только необходимые для этого проекта виды деятельности. Например, проект, полностью разработанный внутри организации, не требует аутсорсинга.

Кроме того, организация выбирает для проекта приложения меры и средства контроля и управления безопасностью приложений.

Данный шаг соответствует «подготовке и реализации планов обработки риска», относящихся к шагу «обработка риска» в устанавливаемом ИСО/МЭК 27005 процессе менеджмента риска.

Примечание — Этот шаг ASMP и его компоненты и процессы более детально представлены в 8.3.

7.3.5 Подготовка к работе и эксплуатация приложений

Четвертым шагом ASMP является фактическое использование мер и средств контроля и управления безопасностью приложений, как предусмотрено ANF в жизненном цикле приложений. Группа проекта реализует меры и средства контроля и управления безопасностью приложений согласно ANF, используя:

a) часть действий по безопасности каждой ASC, осуществляемых соответствующим действующим субъектом, определенным в ASC;

b) часть измерений безопасности каждой ASC, осуществляемых соответствующим действующим субъектом, определенным в ASC.

Этот четвертый шаг соответствует «подготовке и реализации планов обработки риска», относящихся к шагу «обработка риска» в устанавливаемом ИСО/МЭК 27005 процессе менеджмента риска.

Примечание — Этот шаг ASMP и его компоненты и процессы более детально представлены в 8.4.

7.3.6 Проведение аудита безопасности приложений

Пятым и завершающим шагом ASMP является аудит безопасности приложений.

На этом шаге осуществляющая верификацию группа проверяет проведение всех верификационных измерений всеми ASC, включенными в нормативную структуру приложений, а также оценивает достигнутые результаты.

Данный шаг соответствует шагу «мониторинг и проверка» в устанавливаемом ИСО/МЭК 27005 процессе менеджмента риска.

Примечание — Этот шаг ASMP и его компоненты и процессы более детально представлены в 8.5.

8 Общие понятия

8.1 Нормативная структура организации

8.1.1 Общая информация

Нормативная структура организации (ONF) — это структура, позволяющая сохранять признанные организацией лучшие практические приемы безопасности приложений, уточнять или извлекать их. Она включает важнейшие компоненты, процессы, использующие эти компоненты, и процессы менеджмента самой ONF.

ONF представляет собой основу безопасности приложений в организации, на ней базируются все решения организации, связанные с безопасностью приложений. Например, проверка кода может осуществляться как обязательная мера и средство контроля и управления безопасностью приложений только в том случае, если в ONF существует руководство по кодированию.

Как показано на рисунке 3, ONF предоставляет основную входную информацию для ASMP, осуществляемого для каждого проекта приложения в организации.

На рисунке 4 показано высокоуровневое представление контента ONF.

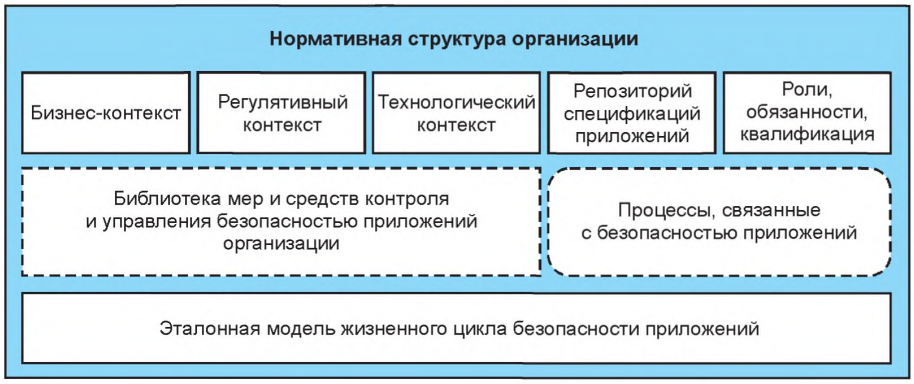

Рисунок 4 — Нормативная структура организации (упрощенная)

Для надлежащего решения вопросов безопасности приложений у организации должна быть формальная ONF, содержащая следующие компоненты:

a) бизнес-контекст;
b) регулятивный контекст;
c) технологический контекст;
d) репозиторий спецификаций приложений;
e) роли, обязанности, квалификация;
f) библиотека ASC организации;
g) процессы, связанные с безопасностью приложений;
h) эталонная модель жизненного цикла безопасности приложений.

Формальная ONF должна также содержать:

a) процесс менеджмента ONF;
b) подпроцессы менеджмента ONF.

8.1.2 Компоненты

8.1.2.1 Бизнес-контекст

Бизнес-контекст перечисляет и документирует все принятые организацией стандарты и лучшие практические приемы, которые могут оказывать влияние на проекты приложений.

Бизнес-контекст включает:

a) процессы менеджмента проекта, разработки, анализа риска, операционные процессы, процессы аудита и контроля;

b) политику безопасности организации;

c) практические приемы в сфере бизнеса;

d) используемую организацией методику разработки;

e) лучшие практические приемы для всех языков программирования, используемых организацией и перечисленных в технологическом контексте;

f) формальный процесс менеджмента проекта организации;

g) применение организацией других необходимых международных стандартов, таких как ИСО/МЭК 27001, ИСО/МЭК 27002 и ИСО/МЭК 15288.

8.1.2.2 Регулятивный контекст

Регулятивный контекст перечисляет и документирует любые законы или предписания в каждом месте ведения бизнеса организацией, которые могут влиять на проекты приложений. Он включает законы, правила и предписания стран или юрисдикций, где разрабатывается и/или развертывается, и/или используется приложение.

Организации, развертывающей и/или использующей одно и то же приложение в разных странах, возможно, придется соответствовать требованиям безопасности каждой страны.

8.1.2.3 Репозиторий спецификаций приложений

Репозиторий спецификаций приложений перечисляет и документирует общие функциональные требования ИТ организации и соответствующие заранее утвержденные решения. Спецификации приложений должны включать:

a) спецификации о том, каким образом приложения будут вычислять, хранить и передавать информацию;

b) обычные параметры приложений, функциональные возможности, услуги и требования;

c) исходный код, двоичный код, библиотеки и продукты или услуги, которые используются приложениями или на которых основаны приложения.

Дополнительные спецификации могут включать подробное описание взаимодействия приложений с:

a) другими системами;

b) рабочей инфраструктурой, от которой они зависят;

c) перечнем мер и средств контроля и управления безопасностью приложений в рабочей среде.

8.1.2.4 Технологический контекст

Технологический контекст содержит инвентарную опись всех продуктов ИТ, услуг и технологий, доступных для проектов приложений организации. Эти продукты, услуги и технологии обуславливают угрозы, которым подвергаются приложения.

Технологический контекст включает компьютеры, инструментальные средства, продукты и услуги ИТ, коммуникационную инфраструктуру и другие технические устройства.

Пример 1 — Технологический контекст, который может оказывать влияние на безопасность приложений, включает инфраструктуру клиент-сервер, веб-инфраструктуру, сетевую инфраструктуру, среду разработки и инструментальные средства разработки.

Технологический контекст также обуславливает введение в приложение определенных мер и средств контроля и управления безопасностью приложений.

Пример 2 — Если технологический контекст не включает механизм аутентификации TLS 1.0[1)] для поддержки функциональности «двусторонняя аутентификация», то ASC на основе TLS 1.0 не могут быть включены в приложение. Группе проекта придется выбирать альтернативные ASC для получения функциональной возможности двусторонней аутентификации, если эта функциональная возможность требуется на целевом уровне доверия приложения.

Технологический контекст должен включать:

a) технологии, доступные для проектов приложений организации.

Инвентарная опись таких технологий должна постоянно обновляться группой ONF через обратную связь от предыдущих проектов приложений;

[1)] TLS (Transport Layer Security) — Протокол безопасности транспортного уровня.

b) технологии, требуемые приложением.

Перечень новых технологий проистекает из новых функциональных требований, определенных в ходе начального планирования проекта приложения. Такие требования должны добавляться в ONF, и организационный процесс должен обеспечивать уверенность в том, что характеристики безопасности технологий, нацеленных на выполнение новых требований, поняты и документально оформлены до утверждения их включения в инвентарную опись технологий организации;

c) доступные технологии.

Данные технологии выявляются в результате исследований, анализа тенденций и мониторинга технологий.

8.1.2.5 Роли, обязанности и квалификация

ONF должна содержать:

a) перечни и описания всех ролей, обязанностей и необходимой профессиональной квалификации всех действующих субъектов, участвующих в создании и поддержке ONF, и/или ролей по созданию и поддержке ASC;

b) перечни и описания всех ролей, обязанностей и необходимой профессиональной квалификации всех действующих субъектов, вовлеченных в жизненный цикл приложений, таких как ответственные за информационную безопасность, руководители проектов, администраторы, лица, занимающиеся приобретением программных средств, руководители разработки программных средств, владельцы приложений, руководители пользователей, разработчики архитектуры, аналитики, программисты, специалисты по тестированию, системные администраторы, администраторы баз данных, сетевые администраторы и технический персонал.

Политика в масштабах организации будет способствовать обеспечению уверенности в том, что все критические роли для всех процессов распределены, все обязанности определены, конфликты интересов предотвращены, а назначенные на роли лица обладают достаточной профессиональной квалификацией.

8.1.2.6 Библиотека ASC организации

8.1.2.6.1 Общие сведения

Организация должна определить, по крайней мере, одну библиотеку мер и средств контроля и управления безопасностью приложений. Эта библиотека называется Библиотекой мер и средств контроля и управления безопасностью приложений (библиотека ASC). В ней перечисляются и документируются все признанные организацией ASC. Эти ASC выводятся из стандартов, лучших практических приемов, ролей, обязанностей и профессиональной квалификации, бизнес-контекста, технологического и регулятивного контекстов, а также спецификаций приложений.

Меры и средства контроля и управления безопасностью приложений в рамках этой библиотеки систематизированы и образуют некоторые совокупности в соответствии с обеспечиваемым ими уровнем защиты от угроз безопасности. Каждая совокупность получает метку, называемую «уровнем доверия», которая информирует руководителей об уровне безопасности, обеспечиваемом конкретной определенной совокупностью мер и средств контроля и управления безопасностью приложений. Если совокупность мер и средств контроля и управления безопасностью приложений описывается как имеющая низкий уровень доверия, то она обеспечивает низкий уровень защиты информационной безопасности. Если совокупность мер и средств контроля и управления безопасностью приложений описывается как имеющая высокий уровень доверия, то она обеспечивает высокий уровень защиты. Уровни доверия описаны далее в 8.1.2.6.4.

Из библиотеки ASC организации выбираются точные и подробные ASC для каждого конкретного проекта приложения.

8.1.2.6.2 Пример библиотеки ASC организации

На рисунке 5 показан простой пример библиотеки ASC организации. Организация в этом примере разрабатывает приложения для авиационной сферы. Библиотека содержит все меры и средства контроля и управления безопасностью приложений, которые нужны организации для реализации функциональных возможностей, лучших практических приемов, стандартов, применяемых законов и предписаний.

В этом примере организация определила две спецификации приложений: безопасное протоколирование и онлайновые платежи. Бизнес-контекстом для данной организации является авиационная сфера, и организация реализует стандарт безопасности данных индустрии платежных карт (PCI-DSS). Регулятивный контекст налагает необходимость соответствия определенным законам обеспечения

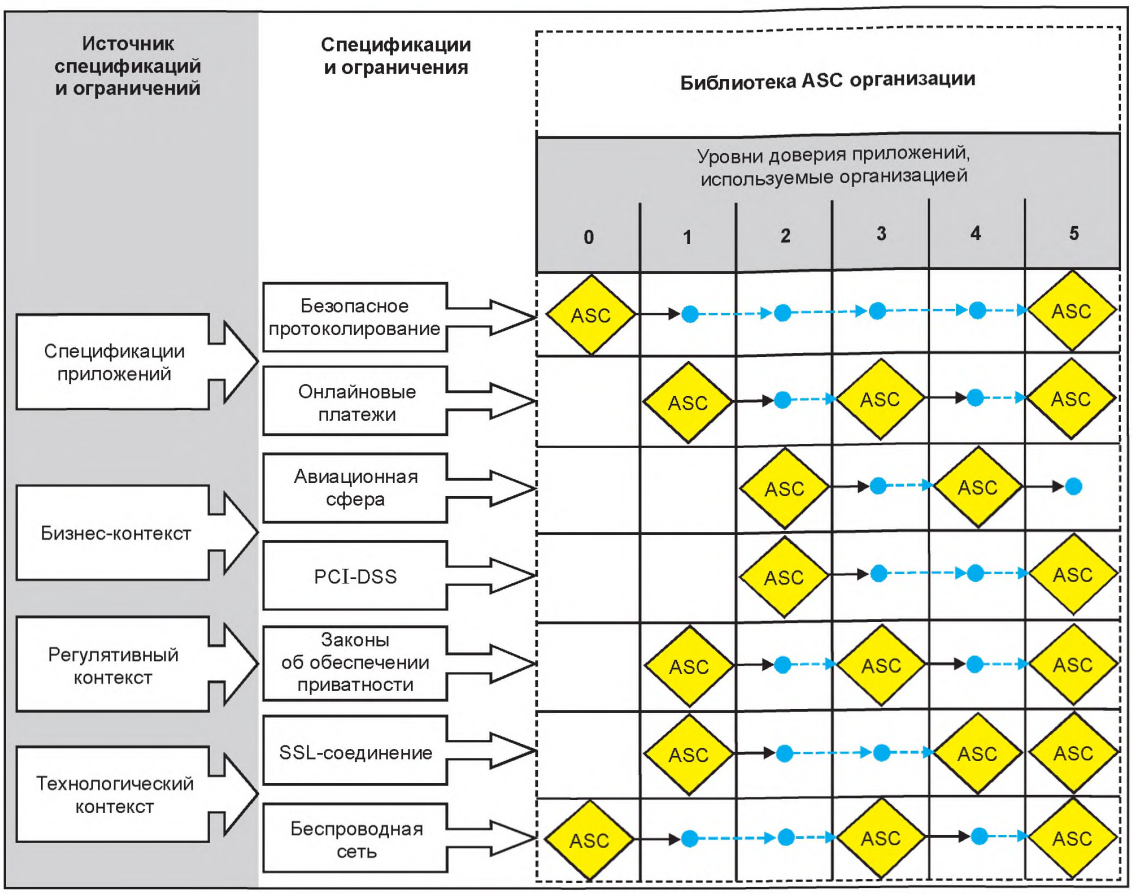

Рисунок 5 — Графическое представление библиотеки ASC организации

приватности. Технологический контекст показывает, что данная организация определила меры и средства контроля и управления для SSL-соединений и беспроводной сети.

Этот простой пример показывает, что спецификации приложений организации, а также ее бизнес-контекст, регулятивный и технологический контексты определяют содержание библиотеки ASC организации. Таким образом, библиотека ASC каждой организации будет специфична для каждой конкретной организации.

8.1.2.6.3 Процесс создания библиотеки ASC организации

Процесс создания библиотеки ASC прост и легко может быть выполнен даже очень небольшими организациями.

Библиотека сначала пуста. ASC добавляются посредством группирования их в графы, соответствующие необходимым уровням доверия (см. графы на рисунке 5). Организации может потребоваться более одного уровня доверия для приложений.

Создание библиотеки ASC, удовлетворяющей конкретным потребностям и требованиям организации, является обязанностью группы ONF.

Библиотека ASC организации может быть создана путем анализа новых или существующих приложений организации. Этот анализ включает определение рисков и требований безопасности для приложений, а затем выбор или создание ASC, отвечающих этим требованиям. Результатом будет совокупность ASC для каждого анализируемого приложения.

Эта совокупность ASC может быть согласована с существующей библиотекой ASC тремя возможными способами:

а) полная совокупность ASC в библиотеке уже обеспечивает требуемый уровень доверия, в таком случае в библиотеку ничего не добавляется;

b) полной совокупности мер и средств контроля и управления безопасностью приложений в библиотеке недостаточно для требуемого уровня доверия, в таком случае библиотека может быть пополнена из новой совокупности ASC;

c) из новой совокупности ASC в библиотеке создается новый уровень доверия.

Таким образом, руководствуясь имеющимся опытом, организация может повторно использовать меры и средства контроля и управления безопасностью от имеющихся приложений или создать/приобрести новые меры и средства контроля и управления, или то и другое вместе.

Библиотека ASC организации расширяется в ответ на замечания и предложения от каждого нового проекта приложения, как описано в 8.1.3.2.

8.1.2.6.4 Уровень доверия приложений

Уровень доверия представляет собой метку, упрощающую взаимодействие действующих субъектов из разных сфер с различными формами обеспечения безопасности приложений в организации. Он определяется организацией с целью однозначной идентификации определенной совокупности мер и средств контроля и управления безопасностью приложений.

Пример 1 — На рисунке 5 организация определила шесть уровней доверия, представленных крайними правыми графами, пронумерованными от 0 до 5.

Пример 2 — На рисунке 5 уровень доверия 1 определяет совокупность из трех ASC, относящихся к онлайновым платежам, законам об обеспечении приватности и SSL-соединениям. Кроме того, на уровне 1 также применяются ASC, относящиеся к безопасному протоколированию и беспроводной сети (показаны стрелками с точкой).

Уровень доверия приложений не является результатом вычислений в отличие от концепции риска, представляющей собой вычисленный результат анализа риска. Соответственно уровень доверия не служит дополнением для риска.

Уровень доверия, скорее, сходен с концепцией плана обеспечения безопасности, представляющего совокупность мер и средств контроля и управления, санкционированных организацией для снижения риска, определенного посредством анализа риска. Таким образом, для каждой организации уровень доверия сходен с заранее определенным и многократно используемым планом обеспечения безопасности.

Организация должна определить собственный диапазон (или область, или шкалу) уровней доверия, который группа ONF должна санкционировать в качестве возможных значений целевого уровня доверия приложений. Этот диапазон может быть определен любым подходящим для организации образом.

Пример 3 — Организация может использовать цифровые уровни от 0 до 5, как в примере на рисунке 5, а может использовать область определенных значений, например [низкий, средний, высокий] или [зеленый, желтый, красный]. Также организация может использовать критерии, основанные на критериях принятия риска.

Организация должна определить минимально допустимый уровень доверия для каждого из своих приложений. В ИСО/МЭК 27034 для идентификации минимально допустимого уровня доверия (в противоположность максимально допустимому риску) используется название «нулевой уровень доверия». Организация может использовать любое название для этого уровня доверия.

Организация должна осуществлять мониторинг уровня доверия, достигнутого приложениями, и применять корректирующие меры, если уровень доверия любого из приложений в какой-то момент падает ниже нулевого уровня доверия, особенно после развертывания приложения.

Пример 4 — На рисунке 5 группа ONF определила ASC с нулевым уровнем доверия для любого приложения, использующего безопасное протоколирование или беспроводную передачу. Даже если целевым уровнем доверия приложения, определенным путем анализа риска для этого приложения, является нулевой уровень доверия, эти ASC должны осуществляться.

8.1.2.6.5 Меры и средства контроля и управления безопасностью приложений

8.1.2.6.5.1 Общие сведения

Меры и средства контроля и управления безопасностью приложений являются главным понятием в ИСО/МЭК 27034. Они используются для введения мероприятий по обеспечению безопасности в жизненный цикл приложений и предоставляют свидетельства, необходимые для проверки их успешного применения.

Понятие мер и средств контроля и управления безопасностью широко используется в сфере информационной безопасности. В ИСО/МЭК 15408-3 и NIST SP 800-53 опубликовано множество соответствующих мер и средств контроля и управления безопасностью, являющихся широкодоступными.

ASC — это используемые в проектах приложений меры и средства контроля и управления безопасностью, определенные с использованием структуры, которая представлена в последующих подпунктах. В приложении В представлен пример, иллюстрирующий, как, используя структуру ASC, можно описать меры и средства контроля и управления безопасностью из NIST SP 800-53.

Для организаций, реализующих концепцию сценариев обеспечения доверия в соответствии с ИСО/МЭК ТО 15026-2, ASC полезны для упрощения менеджмента и своевременного предоставления свидетельств, необходимых для поддержки заявлений и доводов о безопасности приложений. Дальнейшая поддержка доводов обеспечивается последовательным использованием организацией предлагаемых настоящим стандартом процессов по созданию, утверждению и использованию каждой ASC. Поскольку полная совокупность ASC, выбранных для проекта приложения, проистекает из анализа риска безопасности приложений, то она напрямую поддерживает высокоуровневые заявления, обоснования и доводы о безопасности приложений.

ASC могут использоваться для:

a) обеспечения безопасности компонентов приложений, включая программные средства, данные, COTS и инфраструктуру;

b) добавления мероприятий по обеспечению безопасности к процессам, используемым на разных этапах жизненного цикла приложений;

c) проверки ролей, обязанностей и квалификации всех действующих субъектов, вовлеченных в проект;

d) определения критериев для оценивания/приемки компонентов;

e) содействия в определении фактического уровня доверия приложений.

На рисунке 6 показано, что ASC предоставляют группе, работающей над проектом приложения, мероприятия по обеспечению безопасности (т. е. снижение или ограничение конкретного риска безопасности), а группе, занимающейся верификацией, — верификационное измерение (т. е. подтверждение путем изучения подкрепляющих свидетельств, что соответствующее мероприятие обеспечения безопасности успешно осуществлено).

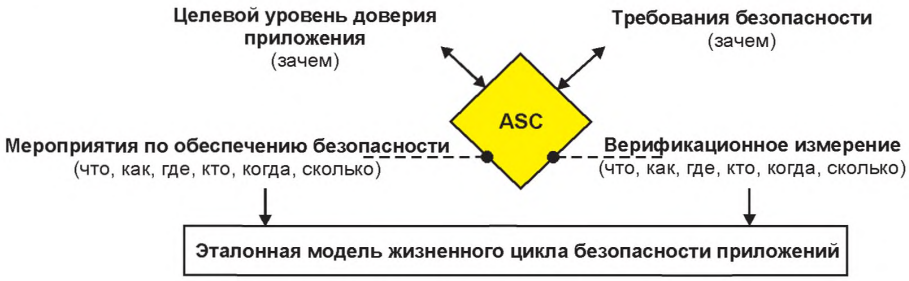

Рисунок 6 — Компоненты ASC

Относящаяся к мероприятиям обеспечения безопасности часть ASC определяет, как решаются вопросы безопасности для проекта приложения.

Относящаяся к измерениям часть ASC определяет, как должны предоставляться свидетельства того, что мероприятие осуществлено надлежащим образом, квалифицированным действующим лицом и что получены ожидаемые результаты.

И мероприятия, и измерения предоставляют сведения о затратах, которые помогут организации в оценивании и утверждении общих расходов на меры и средства контроля и управления безопасностью по отношению к рассматриваемому целевому уровню доверия.

ASC могут быть связаны вместе по схеме так, что после выполнения мероприятий некоторой ASC за ними могут следовать мероприятия дочерних ASC. Это свойство ASC полезно для:

a) предоставления только необходимой информации различным действующим субъектам, скрывая ненужную сложность;

b) облегчения взаимодействия путем группирования соответствующих ASC под определенными заголовками, используя соответствующий словарь, например, используя язык бизнеса при взаимодействии с руководством;

c) содействия распределению ASC путем группирования их во взаимосвязанные совокупности;

d) обеспечения уверенности в том, что все мероприятия по обеспечению доверия в связанных ASC выполнены и ни одно из них не обойдено.

На рисунке 7 показан пример этой схематической связи — совокупность связанных ASC представлена под рубрикой «Онлайновые платежи». В этом примере все связанные с онлайновыми платежами ASC могут использоваться как единая совокупность, и существующая сложность может быть при необходимости скрыта.

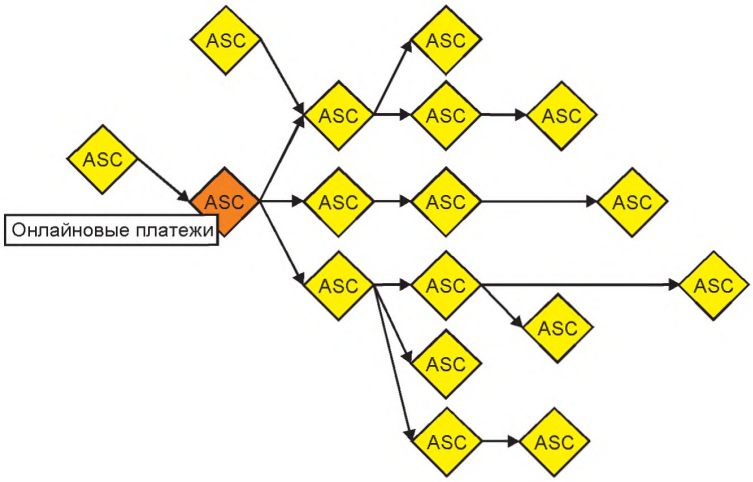

Рисунок 7 — Схема ASC организации

ASC — это сложная структура данных, которая будет детально рассмотрена в ИСО/МЭК 27034-5: «Структура данных управления безопасностью протоколов и приложений». Ниже следует краткий общий обзор ASC.

Примечание — Хотя структура ASC только будет формализована в ИСО/МЭК 27034-5, организации могут по-прежнему обращаться к ИСО/МЭК 15289 за руководством по определению единиц информации, создаваемых во время жизненных циклов приложений.

8.1.2.6.5.2 Идентификация ASC

Элемент идентификации ASC содержит следующее:

a) информацию об ASC: название, идентификатор, автор, дата, описание ASC и т. д.;

b) указатели на материнскую и дочерние ASC (ASC могут быть представлены как схематическая структура);

c) указатели на соответствующий бизнес-контекст, регулятивный и технологический контексты, а также на спецификации приложений, обеспечивающие требования безопасности для данной ASC (см. рисунок 5).

8.1.2.6.5.3 Цель ASC

Цель ASC определяет, «зачем» существует данная ASC, а именно требования безопасности, для реализации которых была разработана данная ASC.

Цель ASC определяет:

a) какие элементы мероприятия по обеспечению безопасности должны создавать подтверждающие свидетельства для соответствующих верификационных измерений;

b) для каких уровней доверия эта ASC является обязательной;

c) спецификации или требования приложений, с которыми связана ASC и которые могут ссылаться на применяемые предписания, стандарты и лучшие практические приемы;

d) угрозы безопасности и предположения об операционной среде приложения.

ASC может быть связана с несколькими уровнями доверия.

Пример — На рисунке 5 ASC определена на уровне доверия 1 для любых приложений, включающих онлайновые платежи. Эта ASC обязательна для любых проектов разработки приложений, включающих онлайновые платежи, где владельцем приложения присвоен целевой уровень доверия от 1 до 2. Если владелец приложения хочет присвоить третий целевой уровень доверия, то нужна ASC с более строгим мероприятием по обеспечению безопасности и/или измерением.

8.1.2.6.5.4 Мероприятие по обеспечению безопасности ASC

Этот элемент описывает шаги или процедуры, необходимые для реализации мероприятия. Он по меньшей мере должен определять:

a) что:

1) полное описание мероприятия по обеспечению безопасности;

2) сложность мероприятия;

3) артефакты, создаваемые в результате мероприятия. Эти артефакты предоставляют свидетельства, подтверждающие наличие процессов или процедур введенной меры и средства контроля и управления безопасностью приложений (т. е. мероприятия по обеспечению безопасности ASC);

4) ожидаемые результаты мероприятий по обеспечению доверия ASC (а именно описание ожидаемой ситуации, состояния или точного значения артефакта, создаваемого в результате мероприятия);

b) как: метод выполнения данного мероприятия и получения артефакта, такого как идентификация исходного кода, использованного для реализации безопасных соединений с сервисом упрощенного протокола доступа к сетевым каталогам (LDAP), идентификация библиотеки, использованной для шифрования, или документ, предоставляющий руководство по выполнению мероприятия;

c) где: цель мероприятия по обеспечению безопасности, такая как исходный код, параметры приложения, компонент инфраструктуры, процесс;

d) кто: необходимая квалификация действующих субъектов, которые должны осуществлять данное мероприятие. Действующие субъекты зависимы от ASC (возможно, в форме официального предписания), потому что организация должна обеспечивать уверенность в достижении необходимой профессиональной квалификации для каждой роли и соблюдении принципа разделения обязанностей. ASC должны быть записаны с точно выраженным назначением проверки профессиональной квалификации;

e) когда: указание на определенную деятельность на этапе эталонной модели жизненного цикла безопасности приложений (см. 8.1.2.7), когда должно осуществляться данное мероприятие;

f) сколько: расчетная стоимость реализации ASC.

8.1.2.6.5.5 Верификационное измерение ASC

Здесь представлено верификационное измерение, проводимое для проверки реализации соответствующей ASC. Верификационное измерение по меньшей мере должно определять:

a) что:

1) полное описание измерения безопасности. Это описание определяет, как верифицируется существование и правильность артефакта, создаваемого в результате реализации ASC;

2) сложность измерения;

3) артефакт, создаваемый при измерении. Этот артефакт предоставляет свидетельства, необходимые для демонстрации верификации ASC;

4) ожидаемые результаты (описание ситуации, состояния или точного значения артефакта);

b) как: метод выполнения данного измерения и получения артефакта, такой как инструментальные средства и установки проверки кода или документ, предоставляющий руководство по выполнению измерения;

c) где: цель верификации, а именно точные характеристики артефакта, создаваемого соответствующей верифицируемой ASC;

d) кто: необходимая профессиональная квалификация действующих субъектов, участвующих в верификации. Действующие субъекты зависимы от ASC (возможно, в форме официального предписания), потому что организация должна обеспечивать уверенность в достижении необходимой профессиональной квалификации для каждой роли и в соблюдении принципа разделения обязанностей. ASC должны быть записаны с точно выраженным назначением проверки профессиональной квалификации;

e) когда: указание на определенную деятельность на этапе эталонной модели жизненного цикла безопасности приложений (см. 8.1.2.7), когда должно осуществляться данное измерение. При необходимости это измерение может осуществляться периодически;

f) сколько: расчетная стоимость выполнения одного верификационного измерения.

8.1.2.7 Эталонная модель жизненного цикла безопасности приложений

8.1.2.7.1 Общая информация

Организация, бизнес которой включает разработку, аутсорсинг или приобретение приложений, обычно использует структуру определенных процессов или деятельности, систематизированную по этапам. Эта структура обычно называется «моделью жизненного цикла». Но в зависимости от контекста ее еще называют «моделью жизненного цикла приложений», либо «моделью жизненного цикла систем», либо «моделью жизненного цикла программных средств». Это не новое понятие, введенное ИСО/МЭК 27034, его определение можно найти в ИСО/МЭК 12207 и ИСО/МЭК 15288.

Такая модель обычно уникальна для конкретной организации и приспособлена к ее требованиям. Она используется и совершенствуется в течение многих лет.

Жизненный цикл определенного приложения, т. е. развитие приложения от замысла до снятия с эксплуатации, представляет собой конкретизацию модели жизненного цикла организации.

В организациях со сложной структурой различные группы, возможно, будут использовать разные модели жизненного цикла приложений для разных проектов. Так часто происходит в крупных децентрализованных организациях или организациях, сформированных путем слияния. В других организациях будут разрабатываться различные специализированные модели жизненного цикла приложений, относящиеся к определенному контексту приложений, например, веб-приложения, приложения, работающие в режиме реального времени, встроенные приложения, медицинские приложения и т. д.

Мероприятия, осуществляемые на различных этапах жизненного цикла программных средств или систем, являются частью процессов в масштабах организации, которые должны соответствовать нормативным требованиям, представленным в ИСО/МЭК 12207 и ИСО/МЭК 15288. Кроме того, в ИСО/МЭК ТО 24748 представлено дополнительное руководство и описаны модели жизненного цикла разработки систем и программных средств, этапы жизненного цикла и их связь с процессами жизненного цикла.

ИСО/МЭК 27034 не рекомендует изменять модели жизненного цикла приложений организации. Вместо этого ИСО/МЭК 27034 рекомендует добавлять к деятельности, обычно выполняемой на этапах определяемой организацией модели жизненного цикла приложений, мероприятия, называемые «мерами и средствами контроля и управления безопасностью приложений» (ASC).

Как ранее отмечалось в 8.1.2.6.5, ASC включают указатели на определенные моменты этапа жизненного цикла, соответственно определяя, «когда» должны выполняться мероприятия по обеспечению безопасности и верификационные измерения.

В настоящее время существует много моделей жизненного цикла программных средств и систем, из которых организация может делать выбор с учетом своих внутренних потребностей. Упоминание их всех или выделение более предпочтительных в ИСО/МЭК 27034 невозможно и нежелательно. Соответственно невозможно включить в стандарт ASC, напрямую указывающую на этап, процесс или мероприятие в конкретной модели жизненного цикла. Это сделало бы концепцию ASC ИСО/МЭК 27034 менее доступной для широкого круга организаций.

В настоящем стандарте представлена эталонная модель жизненного цикла безопасности приложений в качестве стандартизированной ссылки для добавления ASC к мероприятиям, осуществляемым для менеджмента приложений, подготовки к работе и эксплуатации приложений, менеджмента инфраструктуры и аудита приложений. Данная модель является представлением общих этапов и мероприятий, обычно присутствующих в моделях жизненного цикла приложений.

Эталонная модель жизненного цикла безопасности приложений не ограничивается разработкой программных средств. Она также затрагивает мероприятия из других сфер, таких как корпоративное управление, поддержка программных средств и инфраструктуры, менеджмент проектов, аудит и контроль.

Цель эталонной модели жизненного цикла безопасности приложений состоит в:

a) содействии организации в подтверждении правильности каждой модели жизненного цикла ее приложений путем определения всех процессов и действующих субъектов, потенциально вовлеченных в обеспечение безопасности приложений;

b) содействии организации в обеспечении уверенности в том, что вопросы безопасности надлежащим образом рассматриваются на всех этапах жизненного цикла приложений;

c) содействии организации в сведении к минимуму расходов и последствий от введения практических приемов ИСО/МЭК 27034 в ее проекты приложений в качестве поддержки существующих моделей жизненного цикла приложений;

d) предоставлении организации стандартной модели для коллективного использования ASC группами, занимающимися проектами приложений, независимо от различных моделей жизненного цикла приложений;

e) предоставлении организации стандартной модели для коллективного использования ASC вместе с другими организациями, независимо от различных моделей жизненного цикла приложений.

Графическое представление эталонной модели жизненного цикла безопасности приложений, предлагаемой ИСО/МЭК 27034, показано на рисунке 8.



Рисунок 8 — Высокоуровневая эталонная модель жизненного цикла безопасности приложений

Организация должна определить устойчивое соответствие между определенными в этой эталонной модели этапами и мероприятиями, а также этапами и мероприятиями, уже использующимися в каждой из собственных моделей организации. Это дает возможность указать, в какой момент собственных этапов и мероприятий организации применяются ASC.

Группа ONF будет осуществлять распределение ASC в эталонной модели жизненного цикла безопасности приложений. Это распределение будет способствовать обеспечению уверенности в единообразном соблюдении минимально приемлемых ASC для целевого уровня доверия во время начального планирования для каждого проекта приложения организации.

Эта эталонная модель по горизонтали разделяется на два основных этапа: подготовка к работе — осуществляются мероприятия по получению приложения и вводу его в действие, и эксплуатация — осуществляются мероприятия, выполняемые после ввода в действие.

Этапы подготовки к работе и эксплуатации далее делятся на следующие стадии:

a) этап подготовки к работе состоит из трех стадий: подготовка, реализация и ввод в действие;

b) этап эксплуатации состоит из трех стадий: использование и поддержка, архивирование, уничтожение.

Данная эталонная модель по вертикали разделяется на четыре основных уровня:

a) менеджмент приложений: этот уровень составляют мероприятия из сферы корпоративного управления, такие как менеджмент проектов и менеджмент эксплуатации приложений. Такие мероприятия обычно осуществляются в рамках процессов, определенных в СМИБ организации;

b) подготовка к работе и эксплуатация приложений: этот уровень составляют мероприятия, связанные с подготовкой к работе и использованием самого приложения. Такие мероприятия обычно осуществляются в рамках процессов, рекомендуемых ИСО/МЭК 15026, ИСО/МЭК 15288, ИСО/МЭК 12207 и ИСО/МЭК 21827;

c) менеджмент инфраструктуры: этот уровень составляют мероприятия, связанные с менеджментом поддерживающей приложение инфраструктуры услуг ИТ организации. Такие мероприятия обычно осуществляются в рамках процессов, рекомендуемых такими стандартами, как ИСО/МЭК ТО 20000-4, и руководствами, такими как ITIL[1];

d) аудит приложений: этот уровень составляют мероприятия, связанные с контролем и верификацией. Такие мероприятия обычно осуществляются в рамках процессов, рекомендуемых такими стандартами, как ИСО/МЭК 15288, ИСО/МЭК 12207, и документами по отраслевой практике, такими как стандарт CobiT.

Действующими субъектами являются все лица, участвующие на всех этапах всех уровней модели, такие как руководители проектов, разработчики, системные администраторы, администраторы баз данных, руководители пользователей, владельцы приложений, аудиторы, конечные пользователи, технический персонал, обеспечивающий поддержку, сетевые администраторы и т. д.

Мероприятия, обычно осуществляемые на этапах эталонной модели жизненного цикла безопасности приложений, представленной на рисунке 8, описываются ниже.

8.1.2.7.2 Менеджмент подготовки приложений к работе

Мероприятия по менеджменту подготовки приложений к работе осуществляются руководителями проектов и руководителями организации на этапе подготовки к работе жизненного цикла приложений.

Такие мероприятия обычно осуществляются как часть процессов в масштабах организации. Они включают процессы проектирования программных средств из определяемой ИСО/МЭК 12207 группы процессов, связанных с проектами, такие как процесс управления трудовыми ресурсами, процесс планирования проекта, процесс оценки и контроля проекта и процесс управления принятием решений.

8.1.2.7.3 Менеджмент эксплуатации приложений

Мероприятия по менеджменту эксплуатации приложений связаны с менеджментом и использованием приложений на этапе эксплуатации.

Такие мероприятия обычно осуществляются как часть процессов в масштабах организации. Они включают процессы проектирования программных средств из ИСО/МЭК 12207, такие как процесс управления информацией и процесс принятия решений.

Обычно за приложение отвечает его владелец, который может принять решение о разделении части этой ответственности с другими действующими субъектами, такими как руководители пользователей.

Изменения приложений на этапе эксплуатации, например, изменения, проистекающие из новых регулятивных требований или угроз, должны инициироваться владельцем приложений, отвечающим за обеспечение уверенности в том, что приложения надлежащим образом и постоянно учитывают меняющиеся потребности безопасности организации.

Благодаря этим процессам владелец приложений предоставит для СМИБ организации необходимые свидетельства, обеспечивающие уверенность в решении вопросов корпоративного управления проектами приложений.

8.1.2.7.4 Подготовка

На этапе подготовки группа, занимающаяся подготовкой к работе, осуществляет подготовительные мероприятия. Такие мероприятия обычно осуществляются как часть процессов в масштабах организации. Они включают такие процессы проектирования программных средств, как процесс менеджмента решений и процесс менеджмента информации (см. ИСО/МЭК 12207, 6.3.3 и 6.3.6).

8.1.2.7.5 Подготовительные процессы

Подготовительные процессы включают мероприятия, осуществляемые на этапе подготовки проекта приложения.

Примечание — Подготовительные процессы включают процессы проектирования программных средств из ИСО/МЭК 12207, такие как процесс определения требований причастных сторон, анализ требований системы и менеджмент риска (см. ИСО/МЭК 12207, 6.4.1).

---

[1] ITIL (Information Technology Infrastructure Library) — библиотека передового опыта в области информационных технологий.

8.1.2.7.6 Аутсорсинг

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

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

8.1.2.7.7 Разработка

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

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

8.1.2.7.8 Приобретение

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

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

8.1.2.7.9 Ввод в действие

На этапе ввода в действие группой, занимающейся подготовкой к работе, осуществляются мероприятия по подготовке, конфигурированию, тестированию и развертыванию приложения в операционной среде, определяемой организацией.

Такие мероприятия обычно осуществляются как часть процессов в масштабах организации. Они включают процессы проектирования программных средств из ИСО/МЭК 12207, такие как процесс менеджмента конфигурации программных средств, процесс интеграции системы и процесс проверки соответствия системы техническим условиям.

8.1.2.7.10 Использование

На этапе использования и поддержки осуществляются мероприятия, связанные с фактическим использованием приложения в операционной среде всеми пользователями, включая конечных пользователей. Такие мероприятия включают управление доступом пользователей, протоколирование, мониторинг, обучение безопасности и т. д.

С целью сопровождения программных средств и менеджмента изменений осуществляются другие мероприятия, включая обновление прикладного программного средства для выполнения меняющихся информационных требований, например, добавление новых функций и изменение формата данных. Эти мероприятия также включают исправление ошибок и адаптацию программных средств к новым аппаратным устройствам.

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

8.1.2.7.11 Архивирование

Мероприятия по архивированию осуществляются группой, занимающейся эксплуатацией, когда приложение больше уже не нужнó в его активном состоянии. Они включают архивирование всей информации приложения, а также архивирование всех инструментальных средств и процессов для обеспечения защиты и безопасного доступа к этой информации, даже если приложение больше уже не работает в своей операционной среде.

Такие мероприятия обычно осуществляются как часть процессов в масштабах организации. Они включают процессы проектирования программных средств из ИСО/МЭК 12207, например, процесс снятия программных средств с эксплуатации.

8.1.2.7.12 Уничтожение

Мероприятия по уничтожению связаны с безопасным разрушением всей информации приложений, включая данные пользователей, информацию организации, журналы регистрации пользователей, параметры приложений и т. д.

Такие мероприятия обычно осуществляются как часть процессов в масштабах организации. Они включают процессы проектирования программных средств из ИСО/МЭК 12207, например, процесс снятия программных средств с эксплуатации.

8.1.2.7.13 Менеджмент обеспечения инфраструктуры приложений

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

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

8.1.2.7.14 Менеджмент инфраструктуры эксплуатации приложений

Эта сфера деятельности на этапах подготовки к работе включает мероприятия, связанные с обеспечением и поддержанием безопасной технологической инфраструктуры для этапов эксплуатации жизненного цикла приложений. Эти мероприятия охватывают услуги, средства, инструменты и активы информационно-коммуникационной технологии в операционной среде приложений.

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

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

8.1.2.7.15 Снятие с эксплуатации

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

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

8.1.2.7.16 Аудит подготовки приложений к работе

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

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

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

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

8.1.2.7.17 Аудит эксплуатации приложений

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

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

8.1.2.8 Процессы, связанные с безопасностью приложений

ONF представляет собой репозиторий всех используемых организацией процессов. В результате все процессы, связанные с определением, менеджментом и верификацией безопасности приложений, должны иметь надлежащим образом оформленное описание в ONF, включая:

a) все процессы, описанные в разделе 8 настоящего стандарта;

b) все процессы, описанные в последующих частях ИСО/МЭК 27034;

c) все процессы, упоминаемые в ASC, такие как планы реагирования на инциденты, планы обеспечения непрерывности бизнеса, процедуры проверки кода и процедуры тестирования уязвимостей.

8.1.3 Процессы, связанные с нормативной структурой организации

8.1.3.1 Общая информация

Контекст организации развивается с течением времени. В связи с этим следует поддерживать в актуальном состоянии составляющие этот контекст компоненты ONF (например, бизнес-контекст, технологический и регулятивный контексты, а также спецификации приложений).

Группа ONF должна определять, документально оформлять и санкционировать процессы создания, утверждения и поддержки ONF и всех ее компонентов. Должны быть определены роли, обязанности и необходимая профессиональная квалификация всех действующих субъектов, вовлеченных в эти процессы. На рисунке 9 представлен общий обзор процесса, поддерживающего ONF.

Эти процессы упоминаются в настоящем стандарте и будут более детально обсуждаться в ИСО/МЭК 27034-2.

8.1.3.2 Процесс менеджмента ONF

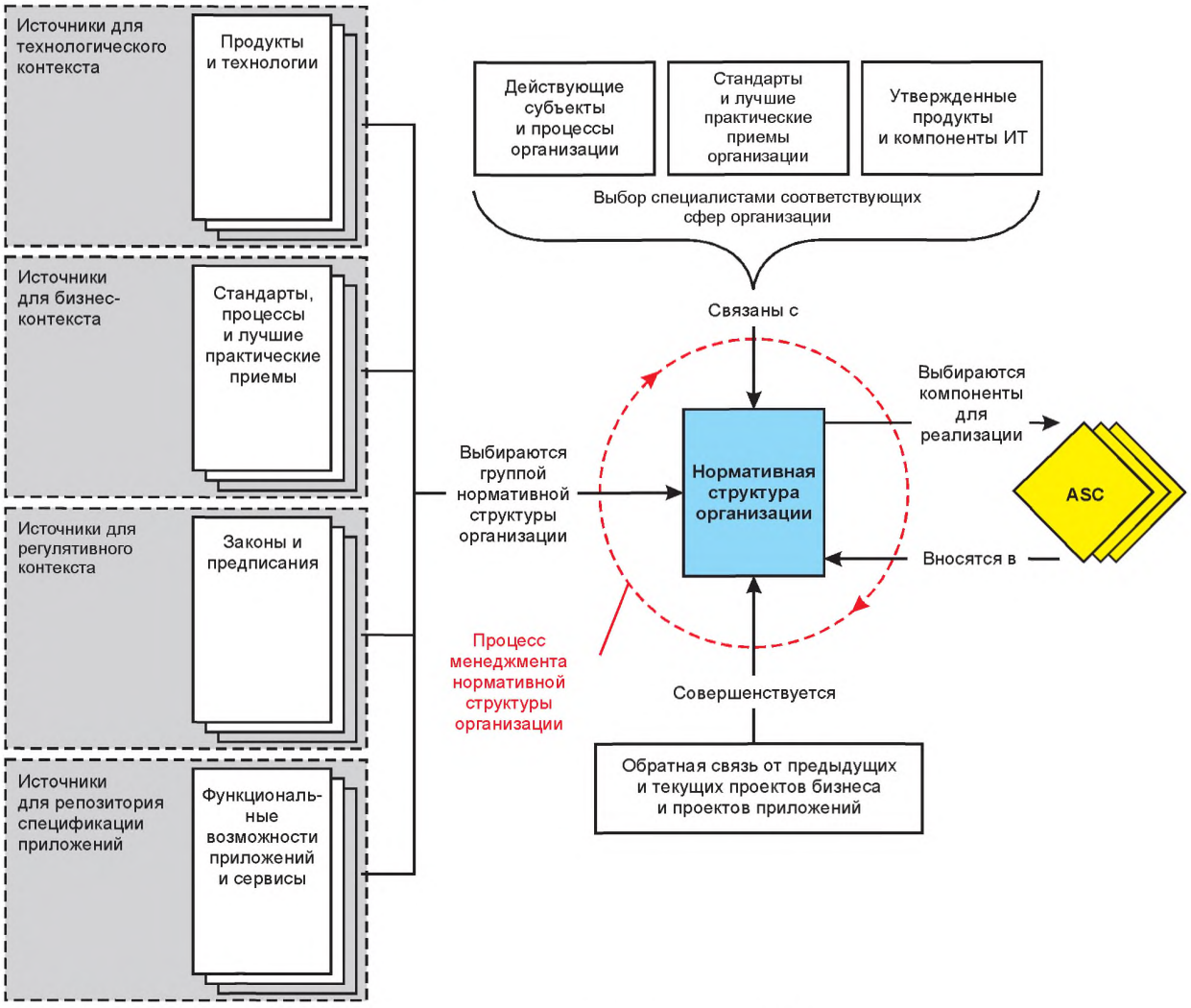

Рисунок 9 — Процесс менеджмента ONF

Процесс менеджмента ONF (рисунок 9) и его подпроцессы представляют собой постоянные процессы в масштабах организации, осуществляемые группой ONF. Как показано на рисунке 3, эти процессы независимы от проектов приложений организации и осуществляются параллельно с ними.

Цели процесса менеджмента ONF:

a) обеспечение уверенности в том, что потребности безопасности приложений, а также утверждение библиотеки ASC и уровней доверия, особенно нулевого уровня доверия, по-прежнему урегулированы с потребностями бизнеса организации;

b) обеспечение уверенности в том, что компоненты ONF обновляются, отражая происходящие вне организации изменения; например, изменения законов могут изменять определенный в ONF регулятивный контекст;

c) утверждение высшим руководством политик безопасности в масштабах организации и признание высшим руководством значимости компонентов ONF;

d) обеспечение уверенности в адекватном и единообразном применении ASC в масштабах организации;

e) информирование о компонентах ONF всех групп в организации;

f) обеспечение обратной связи для ONF с целью включения новых знаний, предложений о совершенствовании ASC и новых практических приемов, приобретенных в ходе осуществления проекта приложения.

8.1.3.3 Подпроцессы менеджмента ONF

Все связанные с безопасностью приложений процессы должны быть частью ONF. Они также должны соответствовать СМИБ организации. В таблице 2 показано, как связанные с безопасностью приложений подпроцессы менеджмента ONF соответствуют четырем этапам процесса СМИБ.

Таблица 2 — Соответствие СМИБ подпроцессам менеджмента ONF, связанным с безопасностью приложений

Процесс СМИБ	**Подпроцесс менеджмента ONF**
Планирование	**Проектирование ONF**
Осуществление	**Реализация ONF**
Проверка	**Мониторинг и проверка ONF**
Действие	**Постоянное совершенствование ONF**

Как показано в таблице 2, процесс менеджмента ONF можно разделить на следующие подпроцессы:

a) проектирование ONF: установление связанных с безопасностью приложений компонентов ONF, включая ASMP, библиотеку ASC и все связанные с ними процессы:

1) определение и документирование возможного контекста (регулятивного, технологического и бизнес-контекста), в котором будет использоваться приложение;

2) создание, документирование и поддержка репозитория спецификаций приложений:

a) анализ спецификаций для каждого нового приложения на этапе поставки;

b) анализ спецификаций существующих в организации приложений;

3) определение действующих субъектов и процессов:

a) анализ и документирование лиц и процессов, вовлеченных в полный жизненный цикл приложений;

b) определение (или разработка) и утверждение формальной методологии анализа риска на уровне приложений, основанной на ИСО/МЭК 27005;

4) анализ лучших практических приемов и стандартов, таких как ИСО/МЭК 12207, ИСО/МЭК 15288 и ИСО/МЭК 15026, и определение на основе этого анализа ASC;

a) создание и обновление ASC.

Создание или обновление ASC для учета конкретных требований безопасности происходит, когда это необходимо организации.

Специалисты в соответствующих сферах должны определять мероприятие по обеспечению безопасности и верификационное измерение, как обсуждалось в 8.1.2.6.5.

Пример 1 — ASC, необходимые для обеспечения безопасности системной программы, должны создаваться или обновляться главным программистом, знающим конкретный язык программирования.

Пример 2 — ASC, необходимые для соблюдения процесса менеджмента идентификаторов приложений, должны создаваться или обновляться специалистом в сфере менеджмента идентификаторов;

b) валидация и интеграция ASC.

Осуществляющая верификацию группа, состоящая из высшего руководства, специалистов-разработчиков, персонала ИТ и аудиторов, должна отвечать за валидацию ASC, обеспечивая уверенность в том, что использующие их лица четко понимают ASC и что данные ASC действительно уменьшают определенный риск. Данная группа также должна определить, для каких заданных уровней доверия требуется данная ASC.

Ответственность за утверждение всех ASC несет группа ONF;

5) анализ, сопоставление с эталонной моделью жизненного цикла безопасности приложений и, в случае необходимости, адаптация текущей модели жизненного цикла приложений организации и других процессов;

6) определение и реализация библиотеки ASC организации;

7) приобретение (или разработка), обновление и валидация необходимых организации ASC, интеграция их в библиотеку ASC;

8) анализ, адаптация и валидация обратной связи от проектов приложений;

b) **реализация ONF:** реализация ONF и информирование о ней;

c) **мониторинг и проверка ONF:** обеспечение уверенности в том, что проекты приложений надлежащим образом используют компоненты ONF, и получение обратной связи от этих проектов:

1) требование наличия целевого уровня доверия и фактического уровня доверия для всех используемых организацией приложений;

2) требование проведения периодической оценки риска для всех используемых организацией приложений;

d) **постоянное совершенствование ONF:** поддержка и совершенствование всех компонентов ONF путем периодической проверки контекста, процессов, лиц и технологии в масштабах организации, обнаружение всех изменений с возможным влиянием на ASMP и интеграции их в ONF.

8.2 Оценка риска безопасности приложений

8.2.1 Оценка риска в сравнении с менеджментом риска

Оценка риска — это второй шаг описанного в ИСО/МЭК 27005 процесса менеджмента риска. Кроме того, оценка риска безопасности приложений является вторым шагом ASMP, применяющего процесс оценки риска на уровне приложений. Другие шаги менеджмента риска осуществляются посредством других шагов ASMP.

Согласно ИСО/МЭК 27005, *«оценка риска определяет ценность информационных активов, идентифицирует применяемые существующие (или могущие существовать) угрозы и уязвимости, идентифицирует существующие меры и средства контроля и управления и их влияние на идентифицированный риск, определяет потенциальные последствия и, наконец, расставляет полученные риски в соответствии с приоритетами и ранжирует их по критериям оценивания риска, определенным на этапе установления контекста».*

Оценка риска включает три действия: идентификацию риска, анализ риска и оценивание риска.

8.2.2 Анализ риска приложений

8.2.2.1 Высокоуровневый анализ риска приложений

Существует высокоуровневый анализ риска, выполняемый на подготовительном этапе жизненного цикла приложений. Такой анализ приблизительно («на глазок») определяет целевой уровень доверия приложений в соответствии с основными спецификациями приложений, бизнес-контекстом, технологическим и регулятивным контекстами приложений.

Владелец конкретного проекта приложения должен четко определить роль, в обязанности которой входит проведение этого анализа с использованием адекватного метода анализа на уровне приложений. Метод анализа риска на уровне организации может не удовлетворять этой задаче.

8.2.2.2 Детальный анализ риска приложений

Этот анализ проводится на этапе реализации жизненного цикла приложений. Он более точно определяет связанные с конкретным приложением остаточные риски, прежде чем рассматривать какие-либо ASC для данного приложения, и подтверждает целевой уровень доверия приложения (определенный во время высокоуровневого анализа риска приложений) в соответствии с детальными спецификациями приложения, бизнес-контекстом, технологическим и регулятивным контекстами организации для приложения.

В результате детального анализа риска приложений владелец приложения может изменить целевой уровень доверия для проекта приложения. Это меняет выбранные для проекта ASC, оказывая влияние на вовлеченных действующих субъектов и расчетную стоимость проекта. Однако это влияние легко предсказуемо, поскольку информация, такая как действующие субъекты, профессиональная квалификация и расчетная стоимость, уже является частью каждой ASC и уже была документирована в библиотеке ASC организации.

Владелец конкретного проекта приложения должен четко определить роль, в обязанности которой входит проведение этого анализа с использованием соответствующего метода анализа на уровне приложений. Метод анализа риска на уровне организации может оказаться не вполне соответствующим для этой задачи.

8.2.3 Оценивание риска

Согласно ИСО/МЭК 27005, *«оценивание риска использует понимание риска, полученное путем анализа риска, для принятия решений о будущих действиях. Решения должны определять:*

a) *следует ли предпринимать действие;*

b) *приоритеты обработки риска, учитывающие оцененные уровни риска».*

В ИСО/МЭК 27034 этот шаг принимает форму выбора целевого уровня доверия приложения, который, в свою очередь, определяет, какие ASC должны быть реализованы для обработки риска.

8.2.4 Целевой уровень доверия приложений

Целевой уровень доверия приложений способствует достижению уровня уверенности, необходимого организации для безопасного использования и развертывания приложения, после принятия остаточных рисков, определенных в результате оценки риска.

Целевой уровень доверия приложения крайне важен для безопасности приложения, поскольку он напрямую определяет соответствующие ASC, которые должны быть выбраны из библиотеки ASC и реализованы во время жизненного цикла приложения.

Процесс оценки риска порождает требования безопасности, устанавливаемые для целевого уровня доверия приложения. Он, в свою очередь, становится целью для группы, работающей над проектом приложения.

Целевой уровень доверия приложения должен быть одним из уровней доверия (или находиться в диапазоне), определенных в библиотеке ASC организации (см. 8.1.2.6), являющейся частью ONF.

Библиотека ASC (см. рисунок 5) может быть представлена в виде таблицы, а целевой уровень доверия приложения — в виде графы в этой таблице. Таким образом, выбор уровня доверия приводит к выбору всех ASC в этой графе.

8.2.5 Принятие риска владельцем приложений

Владелец приложения несет ответственность за принятие остаточных рисков, связанных с конкретным приложением.

Владелец приложения выполняет эту обязанность двумя способами:

a) утверждая целевой уровень доверия приложения на втором шаге ASMP;

b) утверждая результаты аудита безопасности приложений на пятом шаге ASMP, на котором производится измерение фактического уровня доверия приложения и сопоставление его с целевым уровнем доверия приложения. Этот шаг может быть запрошен в любое время владельцем приложения. Для дополнительного подтверждения владелец приложения может потребовать выполнения этого шага внешней группой, осуществляющей верификацию.

После принятия риска владельцем приложения за достижение целевого уровня доверия приложения отвечает группа проекта посредством реализации соответствующих ASC на соответствующих этапах жизненного цикла приложения.

8.3 Нормативная структура приложений

8.3.1 Общая информация

Нормативная структура приложений (ANF) — это подмножество или детализация ONF, содержащей только детальную информацию, которая необходима конкретному приложению для достижения целевого уровня доверия, принятого владельцем приложения в ходе завершающего элемента второго шага ASMP.

Требования безопасности в ANF выводятся из оценки рисков, связанных с использованием приложения организацией, которая осуществляется на втором шаге ASMP.

Для каждого проекта приложения создается ANF, наполняемая соответствующим бизнес-контекстом, технологическим и регулятивным контекстами, спецификациями приложения и соответствующими ASC.

ANF существует в течение жизненного цикла приложения и может развиваться с течением времени. Например, в ходе проекта может меняться регулятивный контекст приложения или владелец приложения может представить новый целевой уровень доверия группе, работающей над проектом приложения. В таких случаях организация может добавлять новые элементы в ANF или убирать их из нее.

Изменения ANF влияют на безопасность приложений. Эти изменения должны соответствующим образом утверждаться владельцем приложения.

ANF для конкретного проекта приложения содержит компоненты, рассмотренные ниже. На рисунке 10 показано графическое представление ANF.

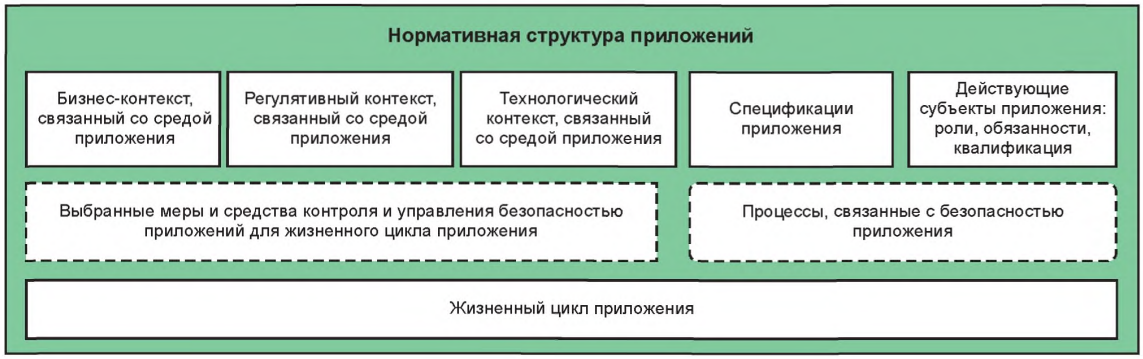

Рисунок 10 — Нормативная структура приложений

8.3.2 Компоненты

8.3.2.1 Бизнес-контекст, связанный со средой приложения

Все процессы бизнеса, методики, стандарты и действующие субъекты, вовлеченные в проект приложения, включая внешние процессы бизнеса, необходимые для обеспечения адекватной целостности бизнеса в операционной среде, выводятся для приложения из бизнес-контекста ONF (см. 8.1.2.1) или детализируются в ней.

8.3.2.2 Регулятивный контекст, связанный со средой приложения

Все правовые и регулятивные требования, применяемые там, где используется или развертывается приложение, выводятся для приложения из регулятивного контекста ONF (см. 8.1.2.2) или детализируются в ней.

8.3.2.3 Технологический контекст, связанный со средой приложения

Все технологические компоненты приложения, такие как его архитектура, инфраструктура, протоколы и языки, выводятся для приложения из технологического контекста ONF (см. 8.1.2.4) или детализируются в ней.

8.3.2.4 Спецификации приложения

Спецификации приложений принимают форму функциональных и нефункциональных требований и требований безопасности.

Должны быть перечислены и распределены по категориям все данные, используемые, хранимые, вычисляемые, разделяемые или передаваемые приложением. В них включаются данные организации, данные пользователей, конфигурационные данные, параметры и иные данные, используемые приложениями. В них также включаются любые выходные данные приложения.

8.3.2.5 Действующие субъекты приложения: роли, обязанности и квалификация

Должны быть определены все действующие субъекты, взаимодействующие с приложением в течение его жизненного цикла. Действующие субъекты включают ответственных за обеспечение безопасности, владельцев приложений, руководителей проектов, аудиторов, разработчиков архитектуры, специалистов по тестированию, разработчиков, конечных пользователей, администраторов, администраторов баз данных и технических специалистов.

8.3.2.6 Выбранные ASC для жизненного цикла приложения

Согласно 8.1.2.6, точные и подробные ASC для конкретного проекта приложения выбираются из библиотеки ASC организации в соответствии с приведенными ниже критериями:

a) целевой уровень доверия приложения;

b) требования организации к приложению;

c) определенный контекст и спецификации приложения.

Каждая ASC представляет собой как мероприятие по обеспечению безопасности, осуществляемое группой проекта приложения для уменьшения конкретного риска безопасности, так и верификационное измерение, осуществляемое занимающейся верификацией группой, для подтверждения, путем изучения подкрепляющих свидетельств, того, что соответствующее мероприятие по обеспечению безопасности успешно выполнено. Каждая ASC также предоставляет указатели на определенные этапы жизненного цикла приложения, на которых должны осуществляться указанное мероприятие по обеспечению безопасности и верификационное измерение.

ASC определяет и утверждает организация до разработки. Разработчикам больше не нужно проектировать их для каждого нового проекта приложения. Это обеспечивает уверенность в унифицированном подходе организации к рассмотрению вопроса требований безопасности приложений.

Выбранные ASC должны, как минимум, включать все ASC, санкционированные группой ONF для нулевого уровня доверия, определенного как минимальный уровень доверия, который примет организация. ASC, санкционированные для нулевого уровня доверия, не должны меняться группой проекта приложения в ходе его разработки.

8.3.3 Процессы, связанные с безопасностью приложения

В ANF должны быть включены все соответствующие процессы, связанные с определением, менеджментом и верификацией безопасности приложений, как описано в ИСО/МЭК 27034. Это детализация компонента «процессы, связанные с безопасностью приложений» нормативной структуры организации, описанного в 8.1.2.8.

8.3.4 Жизненный цикл приложения

Компонент жизненного цикла приложения обозначает этапы и мероприятия, выбранные из ONF для определенного проекта приложения. Более конкретно, жизненный цикл приложений — это подмножество эталонной модели жизненного цикла безопасности приложений (см. 8.1.2.7), содержащейся в ONF.

Жизненный цикл приложений и стандартное содержание эталонной модели жизненного цикла безопасности приложений обсуждались в 8.1.2.7.

Мероприятия и измерения, определяемые ASC, осуществляются посредством различных процессов, выполняемых в течение жизненного цикла приложения, с которыми уже знакомы группы, работающие над проектом и занимающиеся верификацией.

Поэтому предпочтительным подходом является плавная интеграция ASC в качестве составной части в используемые в течение жизненного цикла приложений процессы, а не в качестве отдельных внешних мероприятий по обеспечению безопасности.

8.3.5 Процессы

8.3.5.1 Процессы, связанные с нормативной структурой приложений

Организация должна определять и документально оформлять процессы создания, утверждения и поддержки ANF. Должны быть определены роли, обязанности и необходимая профессиональная квалификация действующих субъектов, связанных с ANF организации для конкретного приложения.

Крайне важен процесс создания ANF для конкретного приложения. Этот процесс преобразует содержащуюся в ONF общую информацию в конкретную информацию, необходимую ANF для определенного приложения и его требований.

Также как ASC в ONF связаны с этапами эталонной модели жизненного цикла безопасности приложений, так и ASC в ANF связаны с этапами жизненного цикла конкретного приложения.

8.3.5.2 Процесс обратной связи

Организация должна определить процесс постоянного совершенствования ONF через обратную связь, обеспечивающую новые знания, предложения по совершенствованию мер и средств контроля и управления безопасностью приложений и практические приемы, приобретенные в ходе разработки и развертывания приложения.

Этот процесс обозначен на рисунке 3 как «Обеспечивает обратную связь для».

Этот процесс должен быть привязан к процессу поддержки ONF, обозначенному на рисунке 9 как «Обратная связь от предыдущих и текущих проектов бизнеса и проектов приложений».

8.4 Подготовка к работе и эксплуатация приложений

8.4.1 Общая информация

Четвертый шаг ASMP включает развертывание специальных ASC, предоставленных ANF, и последующую деятельность в рамках проекта приложения. А именно, группа, работающая над проектом приложения, реализует специальные мероприятия по обеспечению безопасности, описанные в части «Мероприятия по обеспечению безопасности ASC» (см. 8.1.2.6.5.4), для каждой ASC, содержащейся в ANF для данного приложения.

Для группы проекта и группы, занимающейся верификацией, этот шаг упрощается в результате предоставления им только тех ASC, которые требуются для достижения целевого уровня доверия для конкретного проекта. Этим группам не нужно знать процессы, указанные в ANF.

Руководители проектов увидят в ASC эффективное инструментальное средство, потому что в ASC подробно изложены требуемые задачи, ресурсы и квалификация, затраты на каждую задачу в человеко-днях и точный этап жизненного цикла, на котором должна выполняться каждая задача.

Занимающаяся верификацией группа также увидит в ASC эффективное инструментальное средство, поскольку ASC предоставляет подробную информацию о верификационных измерениях, которые должны выполняться для предоставления свидетельств о надлежащем выполнении мероприятий по обеспечению безопасности с ожидаемыми результатами. Это позволит занимающейся верификацией группе удостовериться в том, что приложение отвечает требованиям безопасности посредством формального фиксирования подтверждающих свидетельств.

Группа обеспечения безопасности и технологическая группа также сочтут концепцию ASC полезной, потому что ASC, содержащиеся в ANF для конкретного приложения, предоставляют полный список требований безопасности, позволяя, таким образом, осуществлять заблаговременное планирование необходимых ресурсов.

8.4.2 Влияние ИСО/МЭК 27034 на проект приложения

Типичный проект приложения (до реализации организацией ИСО/МЭК 27034) управляется группой проекта, поддерживается процессами, зачастую на основе автоматизированных технологий, с целью создания приложения. Обычно группа обеспечения качества следует определенному плану тестирования для проверки функциональных возможностей приложения относительно принятых функциональных требований.

Сама технология, методика разработки, используемая группой проекта, зрелость процесса, качество создаваемых артефактов, профессиональная квалификация участвующих в проекте действующих субъектов верифицируются редко, и такие процессы, в случае их выполнения, обычно формально не определяются.

На рисунке 11 показано, как ИСО/МЭК 27034 добавляет новые роли, обязанности, компоненты и процессы в типичный проект приложения.

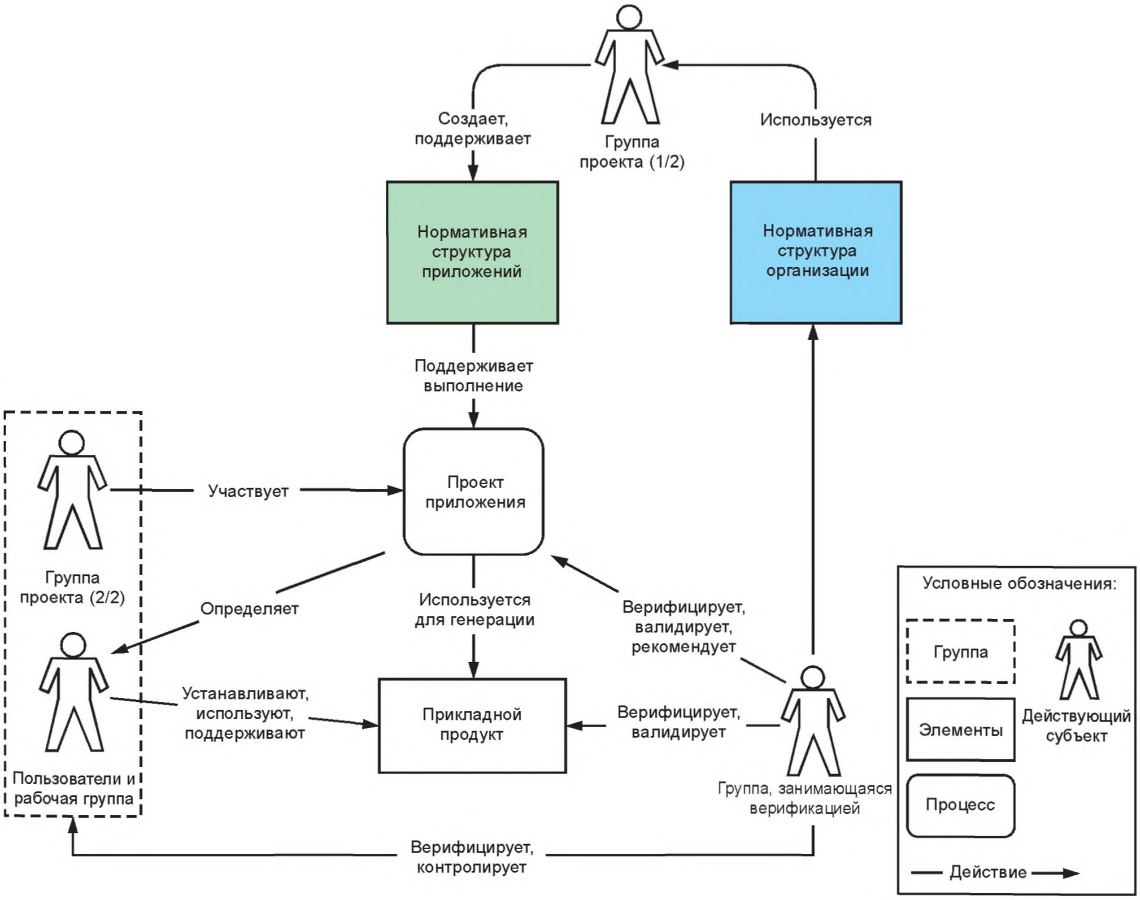

Рисунок 11 — Влияние ИСО/МЭК 27034 на роли и обязанности в типичном проекте приложения

На рисунке 11 показано, как после реализации ИСО/МЭК 27034 будут формально определены роли и обязанности. На нем также показаны два важнейших новых компонента: ONF и ANF. ONF — структура в масштабах организации — не воздействует напрямую на проект приложения. На группу проекта, группу, занимающуюся верификацией, и пользователей будет влиять только ANF, характерная для приложения структура, которая обеспечивает точные и детальные меры и средства контроля и управления безопасностью приложений и соответствующие верификационные измерения.

В обязанности группы, занимающейся верификацией, входит верификация ONF. Это осуществляется не только на уровне проекта (см. 8.4.4.2), но и на уровне организации, как часть процесса менеджмента ONF (см. перечисление d) 8.1.3.3).

8.4.3 Компоненты

8.4.3.1 Группа проекта

Группа проекта состоит из лиц, вовлеченных в проект приложения на этапе подготовки к работе или этапе эксплуатации жизненного цикла приложений, таких как разработчики архитектуры, аналитики, программисты и специалисты по тестированию.

Эти лица отвечают за выбор элементов из ONF для создания или поддержки ANF для проекта приложения.

8.4.3.2 Рабочая группа

Рабочая группа состоит из лиц, участвующих в менеджменте и сопровождении приложения на этапе эксплуатации жизненного цикла приложений, таких как системные администраторы, администраторы баз данных, сетевые администраторы или технические специалисты.

8.4.4 Процессы

8.4.4.1 Выполнение мероприятий безопасности в ходе разработки проекта приложения

На рисунке 12 показано, как группа проекта и рабочая группа используют ASC в качестве инструментального средства для осуществления мероприятий по обеспечению безопасности в ходе разработки конкретного проекта приложения. В проекте будут использоваться только ASC из ANF данного проекта.

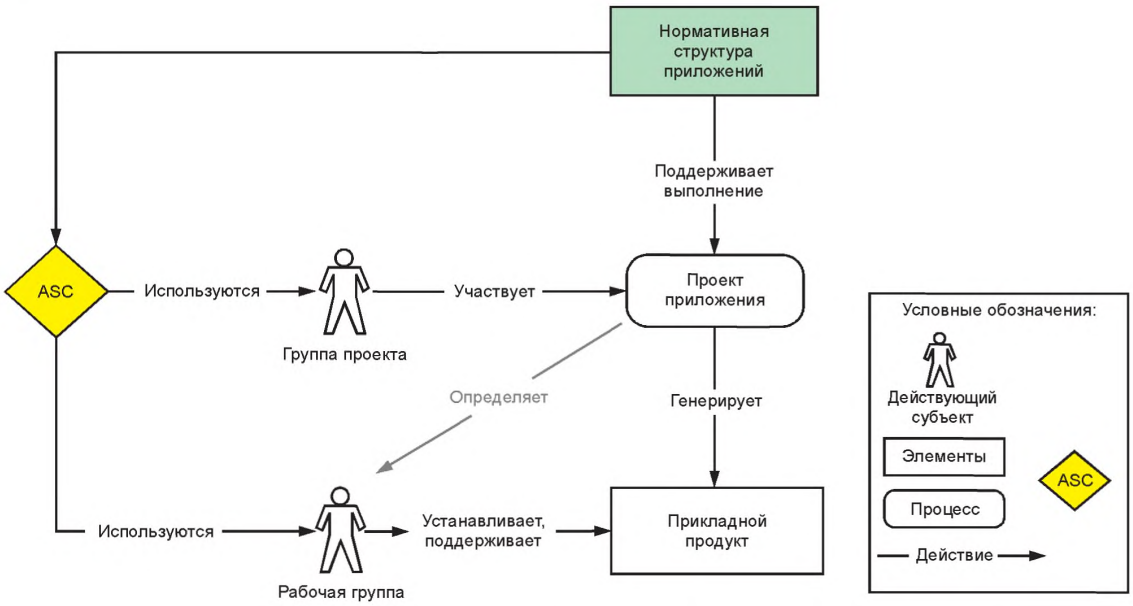

Рисунок 12 — Использование ASC в качестве мероприятий по обеспечению безопасности

8.4.4.2 Проведение верификационных измерений в ходе разработки проекта приложения

Относящаяся к верификационным измерениям часть ASC реализует принцип, состоящий в том, что все мероприятия по обеспечению безопасности должны быть верифицированы с целью предоставления свидетельств того, что мероприятия осуществлены квалифицированным действующим субъектом надлежащим образом и получены ожидаемые результаты.

На рисунке 13 показано, что относящаяся к верификационным измерениям часть мер и средств контроля и управления безопасностью приложений используется как контрольный логический элемент в жизненном цикле проекта приложения, чтобы группа, занимающаяся верификацией, осуществляла верификацию и валидацию приложения и проекта, а также предоставляла рекомендации владельцу приложения для принятия решения о санкционировании перехода проекта приложения к следующему шагу его выполнения. Например, ASC могут потребовать использования услуги кластеризации серверов для обеспечения доступности приложения. Относящаяся к верификационным измерениям часть ASC проверяет, действительно ли такая услуга реализована надлежащим образом.

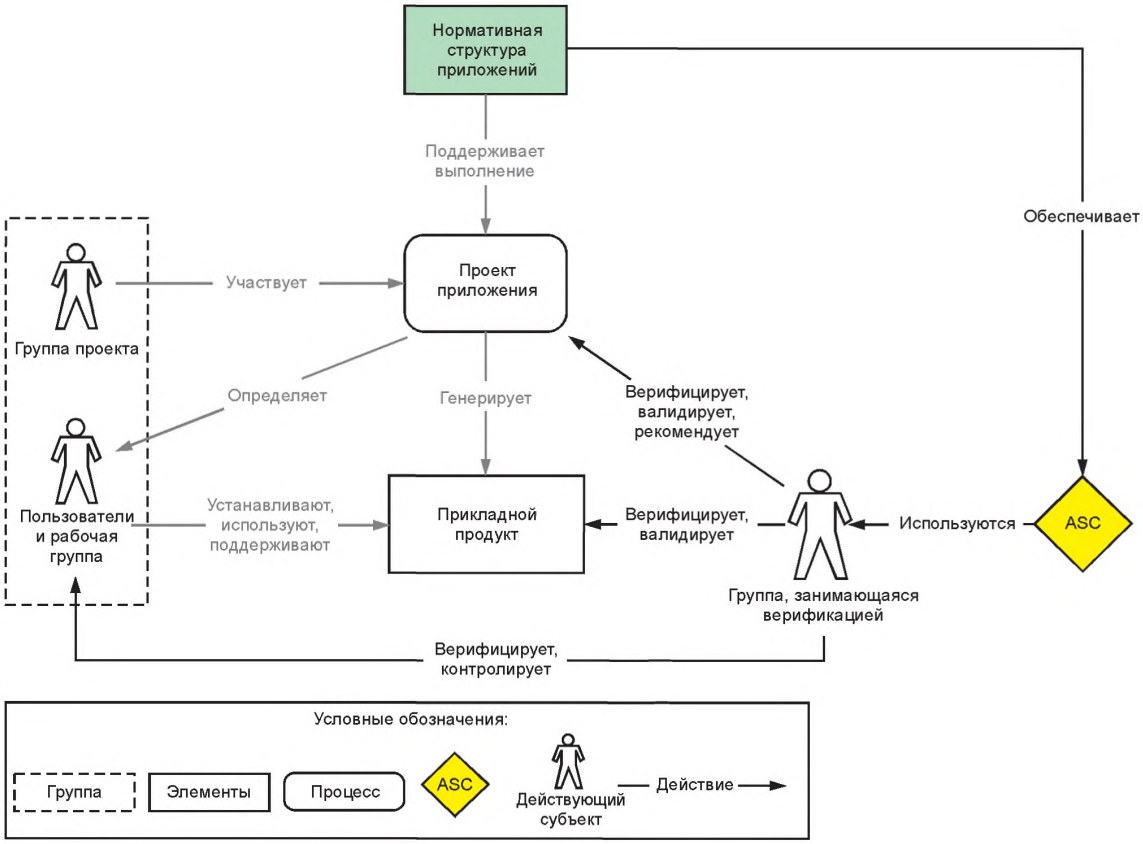

Рисунок 13 — Использование ASC в качестве измерений

На рисунке 13 также показано, что относящаяся к верификационным измерениям часть ASC может использоваться для верификации квалификации действующих субъектов, осуществляющих мероприятия жизненного цикла приложения. Например, ASC могут потребовать, чтобы критический компонент приложения реализовывал главный разработчик. Относящаяся к верификационным измерениям часть ASC проверяет квалификацию разработчика, реализовавшего этот компонент.

8.5 Аудит безопасности приложений

8.5.1 Общая информация

Цель данного пятого шага ASMP состоит в верификации и формальном фиксировании подтверждающих свидетельств достижения и поддержания конкретным приложением целевого уровня доверия приложения.

Данный шаг ASMP может выполняться в любое время в течение жизненного цикла приложения. В зависимости от целевого уровня доверия приложения этот шаг может быть однократным, периодическим или обуславливаемым событиями.

Пример 1 — Организация может периодически выполнять этот шаг для мониторинга степени обеспечения безопасности на этапе реализации приложения.

Пример 2 — Организация может выполнять этот шаг для демонстрации фактического уровня доверия приложения, прежде чем будет утверждено его развертывание.

Пример 3 — Организация может выполнять этот шаг на этапе эксплуатации жизненного цикла приложения как часть ежегодно проводимого организацией аудита безопасности.

В рамках этого шага внутренняя или внешняя группа, занимающаяся верификацией (в зависимости от политик организации, содержащихся в ONF), проверяет, чтобы все верификационные измерения, представленные всеми ASC в ANF для конкретного приложения, были выполнены и результаты верифицированы. Целью данного шага является демонстрация в определенное время фактического уровня доверия приложения. Организация может объявить приложение «безопасным», когда его фактический уровень доверия равен его целевому уровню доверия.

Этот шаг соответствует шагу «принятие риска» в устанавливаемом ИСО/МЭК 27005 процессе менеджмента риска.

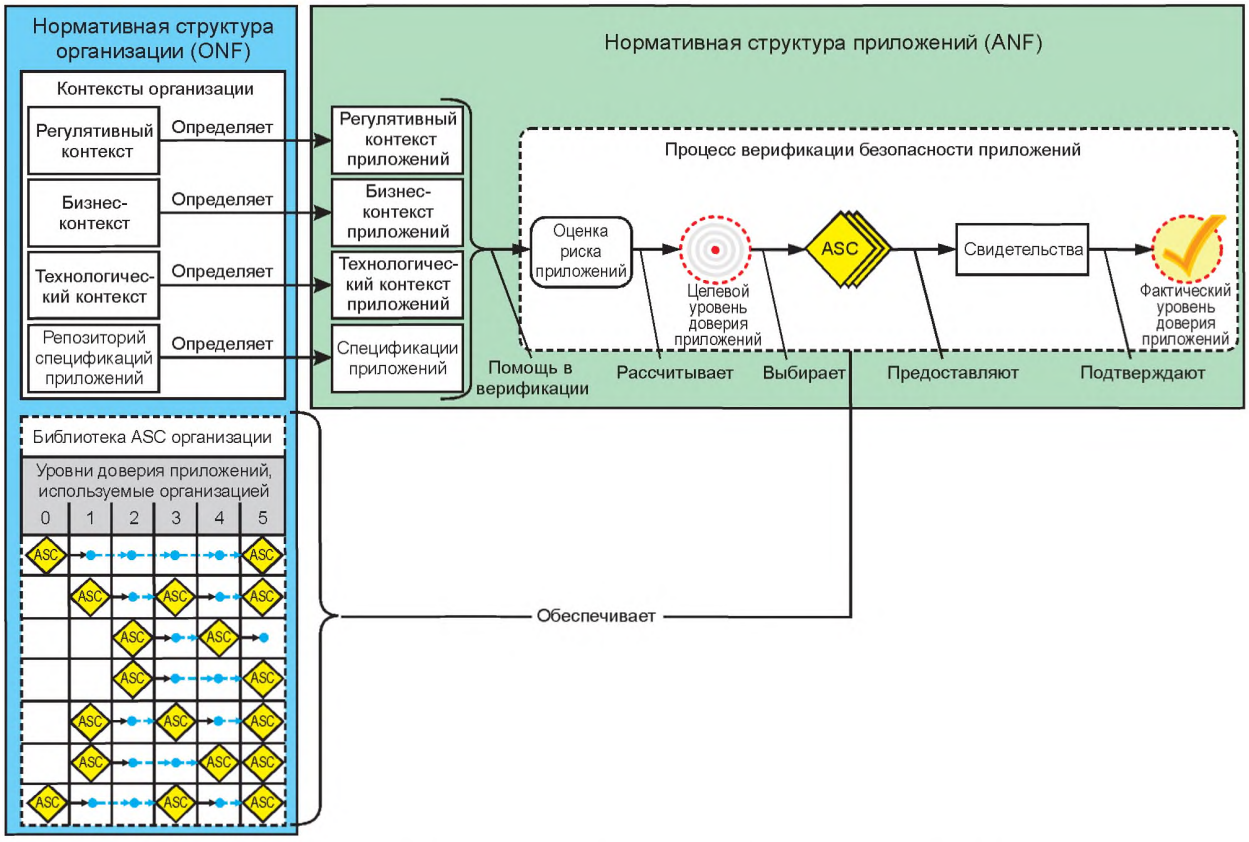

Рисунок 14 — Общий обзор процесса верификации безопасности приложений

8.5.2 Компоненты

8.5.2.1 Фактический уровень доверия приложений

Фактический уровень доверия приложения — это максимальный уровень уверенности, демонстрируемый группой, занимающейся верификацией, на основе верификационных измерений всех ASC для данного приложения.

Каждая ASC, включенная в ANF для какого-либо проекта приложения, предусматривает конкретные и детальные измерения, которые должны выполняться группой, занимающейся верификацией, наряду с указателями на определенный этап жизненного цикла приложений, во время которого должно выполняться измерение.

Фактический уровень доверия приложений получают путем верификации ASC, которая должна быть осуществлена в конкретный момент жизненного цикла приложений. Если какая-либо ASC не проходит верификацию, организация должна принять соответствующие меры для исправления ситуации.

Успешное достижение целевого уровня доверия приложения подтверждается в случае успешного выполнения верификации подтверждающих свидетельств, полученных в результате верификационных измерений всех запланированных ASC.

После такого подтверждения организация считает приложение безопасным для использования или развертывания с данного момента до момента следующей верификации, предписываемой требованием периодической проверки в рамках пятого шага ASMP или другими требованиями организации.

Приложение А
(справочное)

Пример сопоставления существующего процесса разработки с ИСО/МЭК 27034

А.1 Общая информация

Цель данного приложения — проиллюстрировать на примере, как фактически существующий сосредоточенный на безопасности процесс разработки программных средств (SDL) можно с успехом сопоставить с некоторыми компонентами и процессами ИСО/МЭК 27034.

Если специально не отмечено иное, то данный конкретный пример предполагает, что все обсуждаемые мероприятия и результаты деятельности соответствуют ИСО/МЭК 27034.

В данном приложении в поддержку ИСО/МЭК 27034 приведены:

a) краткий обзор жизненного цикла разработки безопасного программного обеспечения;

b) сопоставление практических приемов обеспечения безопасного программного обеспечения с нормативной структурой организации. В частности, в данном приложении:

1) объясняются взаимосвязи между бизнес-контекстом, технологическим и регулятивным контекстами;
2) обсуждаются процессы создания и поддержки спецификаций приложений;
3) в общих чертах описываются роли и обязанности различных лиц, вовлеченных в процесс разработки приложения;
4) приводятся существующие меры и средства контроля и управления безопасностью приложений (ASC);
5) обсуждается процесс верификации безопасности приложений;
6) дается наглядная иллюстрация эталонной модели жизненного цикла безопасности приложений;
7) даются примеры дополнительных мероприятий, выполнение которых может потребоваться организации, использующей SDL, для соответствия ИСО/МЭК 27034.

Для удобства рассмотрения описания мер и средств контроля и управления безопасностью приложений, приведенных в настоящем стандарте, помещены в текстовых окнах в приведенных ниже подразделах, за каждым из них следует пример применения.

Где возможно, приводятся ссылки на общедоступные источники информации; в настоящем стандарте можно найти веб-ссылки на конкретное обсуждение процессов, инструментальных средств и иную дополнительную информацию.

Важно отметить, что создатели данного приложения решили сосредоточиться *исключительно на методике разработки безопасных программных средств, используемой для поставки коммерческого прикладного программного средства и онлайновых услуг.* Существуют другие процессы, охватывающие задачи безопасности ИТ. Группы, администрирующие эти процессы, связаны аналогичным технологическим и регулятивным контекстами, но не создают прикладное программное средство, предназначенное для широкого общественного использования. Хотя иллюстрация методик разработки безопасных программных средств и ИТ может показаться интересной для некоторых читателей, она не обязательно предоставит более убедительные свидетельства практичности ИСО/МЭК 27034.

Использование жизненного цикла разработки безопасного программного средства (Security Development Lifecycle — SDL) в этом поясняющем контексте не означает одобрение SDL Международной организацией по стандартизации (ИСО).

А.2 О жизненном цикле разработки безопасного программного средства

Жизненный цикл разработки безопасного программного средства (SDL) — это процесс обеспечения доверия к безопасности программных средств. Используемый в качестве инициативы в масштабе компаний и обязательной политики с 2004 года, SDL сыграл важную роль во встраивании обеспечения безопасности и приватности в программные средства и культуру принимающей его компании. Сочетая целостный и практичный подход, SDL вводит безопасность и приватность во все этапы процесса разработки. Ссылки на частные технологии и ресурсы в данном приложении опущены.

Как показано на рисунке А.1, жизненный цикл разработки безопасного программного средства состоит из семи этапов.



Рисунок А.1 — Жизненный цикл разработки безопасного программного средства

А.3 Сопоставление SDL с нормативной структурой организации

Сопоставление SDL с нормативной структурой организации показано на рисунке А.2. Последующее обсуждение SDL будет придерживаться этого формата.



Рисунок А.2 — Сопоставление SDL с нормативной структурой организации

Список сокращений:

PG	product group (группа продуктов);
LCA	legal and corporate affairs (правовые и корпоративные вопросы);
LOB App	proprietary line of applications used in support of business and technological contexts (характерные особенности приложений, используемые в поддержку бизнес-контекста и технологического контекста);
SDL	security development lifecycle (жизненный цикл разработки безопасного программного средства);
HR	human resources (кадровый отдел);
FSR	final security review (окончательная проверка безопасности).

А.4 Бизнес-контекст

8.1.2.1 Бизнес-контекст перечисляет и документирует все принятые организацией стандарты и лучшие практические приемы, которые могут оказывать влияние на проекты приложений.

Бизнес-контекст включает:

a) процессы менеджмента проекта, разработки, анализа риска, операционные процессы, процессы аудита и контроля;

b) политику безопасности организации;

c) практические приемы в сфере бизнеса;

d) используемую организацией методику разработки;

e) лучшие практические приемы для всех языков программирования, используемых организацией и перечисленных в технологическом контексте;

f) формальный процесс менеджмента проекта организации;

g) применение организацией других необходимых международных стандартов ИСО/МЭК, таких как ИСО/МЭК 27001, ИСО/МЭК 27002 и ИСО/МЭК 15288.

Бизнес-контекст определяется сочетанием общих корпоративных политик, специальных (частных) политик, технического контекста и движущих рыночных факторов отдельных организационных единиц в рамках корпорации.

Приватность и безопасность при разработке программных продуктов является *общекорпоративным* предписанием согласно жизненному циклу разработки безопасного программного средства (SDL).[i 1)] SDL также требует определения лиц (руководящих обеспечением безопасности и приватности), процессов и мер и средств контроля

[1)] Таким образом (здесь и далее по тексту приложения А) нумеруется ссылка, приведенная в конце приложения А.

и управления безопасностью приложения, которые будут использоваться для отслеживания продвижения к целям обеспечения безопасности и приватности[ii].

Учитывая широкий спектр сценариев и платформ разработки, обязательное строгое соблюдение фиксированной совокупности методик разработки или инструментальных средств невыполнимо. Поэтому группам бизнеса разрешено обращаться по техническим проблемам, не охваченным напрямую политикой SDL (например, компиляторы и инструментальные средства на различных платформах), к специалистам по конкретным вопросам безопасности для консультации (см. А.8).

А.5 Регулятивный контекст

8.1.2.2 Регулятивный контекст перечисляет и документирует любые законы или предписания в каждом месте ведения бизнеса организацией, которые могут влиять на проекты приложений. Он включает законы, правила и предписания стран или юрисдикций, где разрабатывается, и/или развертывается, и/или используется приложение.

Организации, развертывающей и/или использующей одно и то же приложение в разных странах, возможно, придется соответствовать требованиям безопасности каждой страны.

Проверка соответствия регулятивным требованиям и геополитический анализ охватывают существующие бизнес-процессы и упреждающим образом используются для информирования групп проекта. Бизнес-подразделениями и отделом правовых и корпоративных вопросов анализируются политики для обеспечения уверенности в том, что все аспекты создания и выпуска программных средств соответствуют любым *известным* правовым или регулятивным критериям, существующим в различных регионах мира, и что любые новые проекты действуют в рамках границ существующих мандатов политики.

Ряд приложений (в сочетании с упомянутыми выше проверками) используется группами, отвечающими за продукт, для автоматизации процесса обеспечения соответствия регулятивным требованиям для прикладного программного средства, разработанного для публичного выпуска.

Наконец, результаты регулятивных и геополитических проверок находятся в архивах вместе с результатами процесса верификации безопасности приложений (который обсуждается ниже) для создания объективного и всестороннего представления процесса разработки безопасных приложений. Однако важно отметить, что *регулятивные и геополитические политики не предназначены для жизненного цикла разработки безопасного программного средства.*

А.6 Репозиторий спецификаций приложений

8.1.2.3 Репозиторий спецификаций приложений перечисляет и документирует общие функциональные требования ИТ организации и соответствующие, заранее утвержденные решения. Спецификации приложений должны включать:

a) спецификации о том, каким образом приложения будут вычислять, хранить и передавать информацию;

b) обычные параметры приложений, функциональные возможности, услуги и требования;

c) исходный код, двоичный код, библиотеки и продукты или услуги, которые используются приложениями или на которых основаны приложения.

Дополнительные спецификации могут включать подробное описание взаимодействия приложений с:

a) другими системами;

b) рабочей инфраструктурой, от которой они зависят;

c) перечнем мер и средств контроля и управления безопасностью приложений в рабочей среде.

Спецификации создаются и хранятся отдельными бизнес-подразделениями и обычно состоят из функциональных указаний (описывающих, как определенный компонент должен вычислять, хранить и передавать информацию) и технических указаний (определяющих языки программирования, компиляторы, библиотеки и т. д.). В некоторых случаях SDL устанавливает политику для компонентов или других технологий, имеющих контекст безопасности (например, библиотеки криптографических сервисов), с целью обеспечения уверенности в том, что приватность и безопасность приложений не компрометируются функциональными требованиями или возможностями.

А.7 Технологический контекст

8.1.2.4 Технологический контекст содержит инвентарную опись всех продуктов ИТ, услуг и технологий, доступных для проектов приложений организации. Эти продукты, услуги и технологии обуславливают угрозы, которым подвергаются приложения.

Технологический контекст включает компьютеры, инструментальные средства, продукты и услуги ИТ, коммуникационную инфраструктуру и другие технические устройства.

Пример — Технологический контекст, который может оказывать влияние на безопасность приложений, включает инфраструктуру клиент-сервер, веб-инфраструктуру, сетевую инфраструктуру, среду разработки и инструментальные средства разработки.

Технологический контекст часто различается среди бизнес-подразделений, он выводится из комбинации движущих рыночных факторов, сценариев возможности взаимодействия и совместимости и технических стандартов для конкретной группы. В связи с разнообразием используемых среди бизнес-подразделений стандартов для продуктов ИТ, услуг и технологий, технологический контекст каждым бизнес-подразделением устанавливается независимо, чтобы он мог отвечать их потребностям. Однако бизнес-подразделения должны также обеспечивать уверенность в том, что связанные с программными средствами проекты используют услуги ИТ и технологии, позволяющие им удовлетворять критериям безопасности и приватности, устанавливаемым бизнес-контекстом и регулятивным контекстом.

А.8 Роли, обязанности и квалификация

8.1.2.5 ONF должна содержать:

a) перечни и описания всех ролей, обязанностей и необходимой профессиональной квалификации всех действующих субъектов, участвующих в создании и поддержке ONF, и/или ролей по созданию и поддержке ASC;

b) перечни и описания всех ролей, обязанностей и необходимой профессиональной квалификации всех действующих субъектов, вовлеченных в жизненный цикл приложений, таких как ответственные за информационную безопасность, руководители проектов, администраторы, лица, занимающиеся приобретением программных средств, руководители разработки программных средств, владельцы приложений, руководители пользователей, разработчики архитектуры, аналитики, программисты, специалисты по тестированию, системные администраторы, администраторы баз данных, сетевые администраторы и технический персонал.

Политика в масштабах организации будет способствовать обеспечению уверенности в том, что все критические роли для всех процессов распределены, все обязанности определены, конфликты интересов предотвращены, а назначенные на роли лица обладают достаточной профессиональной квалификацией.

Категории (разряд) работы персонала создаются и поддерживаются кадровой службой, получающей входную информацию от бизнес-подразделений. Эти категории включают высокоуровневое описание задач и компетентности, характерных для каждой рабочей роли. В то время как кадровая служба поддерживает общие должностные инструкции, бизнес-подразделения обычно отвечают за принятие решений о том, как конкретно определить категории работы в отношении компетентности в сфере обеспечения безопасности и приватности и использовать эти критерии для содействия делегированию обязанностей по надзору за обеспечением безопасности в рамках группы, занимающейся разработкой.

В SDL есть общие критерии и должностные инструкции для ролей по обеспечению безопасности и приватности; эти роли назначаются на этапе «Требования» процесса SDL.[iii] Это специальные рабочие роли, которые должны быть определены до начала этапа разработки. Эти роли являются консультационными по своему характеру и обеспечивают основу, необходимую для идентификации, классификации и уменьшения проблем безопасности и приватности, имеющихся в проекте разработки программных средств. Эти роли включают:

Надзорные роли: Данные роли предназначены для обеспечения надзора за проектом и могут включать как количественные, так и качественные рекомендации группе проекта в отношении минимально допустимых порогов доверия к безопасности и приватности для проекта, связанного с программными средствами. Надзорные роли должны быть также наделены полномочиями принятия или отклонения планов обеспечения безопасности и приватности, поступающих от группы проекта.

a) **Куратор по обеспечению безопасности:** На данную роль назначают специалиста по отдельным вопросам безопасности, являющегося внешним для группы проекта. Эту роль может выполнять квалифицированный представитель независимой централизованной группы обеспечения безопасности в рамках организации или можно обращаться к услугам внешнего специалиста. Лицо, выбранное для решения этой задачи, должно выполнять две функции:

i) аудитора, т. е. осуществлять мониторинг безопасности каждого этапа процесса разработки и подтверждать успешное выполнение требований каждого этапа, а также обладать свободой в вопросе подтверждения соответствия (или несоответствия) требованиям безопасности без вмешательства со стороны группы проекта;

ii) эксперта, т. е. обладать поддающейся проверке компетентностью в вопросах безопасности;

b) **Куратор по обеспечению приватности:** На данную роль назначают специалиста по отдельным вопросам приватности, являющегося внешним по отношению к группе проекта. Эту роль может выполнять квалифицированный представитель независимой централизованной группы обеспечения приватности в рамках организации или можно обращаться к услугам внешнего специалиста. Лицо, выбранное для решения этой задачи, должно выполнять две функции:

i) аудитора, т. е. осуществлять мониторинг приватности каждого этапа процесса разработки и подтверждать успешное выполнение требований каждого этапа, а также обладать свободой в вопросе подтверждения соответствия (или несоответствия) требованиям приватности без вмешательства со стороны группы проекта;

ii) эксперта, т. е. обладать поддающейся проверке компетентностью в вопросах приватности.

Комбинация кураторских ролей: Роль куратора по обеспечению безопасности может быть объединена с ролью куратора по обеспечению приватности при условии, что может быть определено лицо с соответствующими навыками и опытом.

Руководители групп: Данные роли должны выполняться специалистами в соответствующей области, которые будут представлять группу разработки проекта на обсуждениях с кураторами по обеспечению безопасности и приватности. Эта роль отвечает за обсуждение, принятие и отслеживание минимальных требований безопасности и поддержку четкой связи с кураторами и другими принимающими решениями лицами во время работы над проектом по разработке программных средств.

a) **Руководители группы по вопросам безопасности:** Это лицо (или группа лиц) не несет единоличной ответственности за обеспечение уверенности в том, что выпуск программного продукта учитывает все вопросы безопасности, однако оно отвечает за координацию и отслеживание вопросов безопасности для проекта. Лицо, выполняющее эту роль, также несет ответственность за состояние отчетности перед куратором по обеспечению безопасности и другими заинтересованными сторонами (например, руководителями разработки и тестирования) из группы проекта;

b) **Руководители группы по вопросам приватности:** Это лицо (или группа лиц) не несет единоличной ответственности за обеспечение уверенности в том, что выпуск программного продукта учитывает все вопросы приватности, однако оно отвечает за координацию и отслеживание вопросов приватности для проекта. Лицо, выполняющее эту роль, также несет ответственность за состояние отчетности перед куратором по обеспечению приватности и другими заинтересованными сторонами (например, руководителями разработки и тестирования) из группы проекта.

A.9 Библиотека ASC организации

8.1.2.6 Организация должна определить, по крайней мере, одну библиотеку мер и средств контроля и управления безопасностью приложений. Эта библиотека называется Библиотекой мер и средств контроля и управления безопасностью приложений (библиотека ASC). В ней перечисляются и документируются все признанные организацией ASC. Эти ASC выводятся из стандартов, лучших практических приемов, ролей, обязанностей и профессиональной квалификации, бизнес-контекста, технологического и регулятивного контекстов, а также спецификаций приложений.

Как часть иллюстрируемого ниже процесса SDL было идентифицировано семнадцать ASC. Этот пример включает как обязательные, так и необязательные задачи. Необязательные задачи ASC могут добавляться бизнес-подразделениями в случае необходимости достижения желаемых целей безопасности и приватности. ASC, изображенные на рисунке А.3, представлены в порядке их появления с использованием традиционной каскадной модели разработки. Для краткости полное обсуждение каждой ASC опущено.

Крайняя слева ASC может считаться «корневой» ASC — по существу «родительским узлом» детальной древовидной схемы ASC, показанной на рисунке А.3. Эта иллюстрация показывает, что организация может применять ASC с возрастающими уровнями сложности и детальности, чтобы соответствовать целевому уровню доверия для приложения, который организация выбирает до начала проекта приложения.

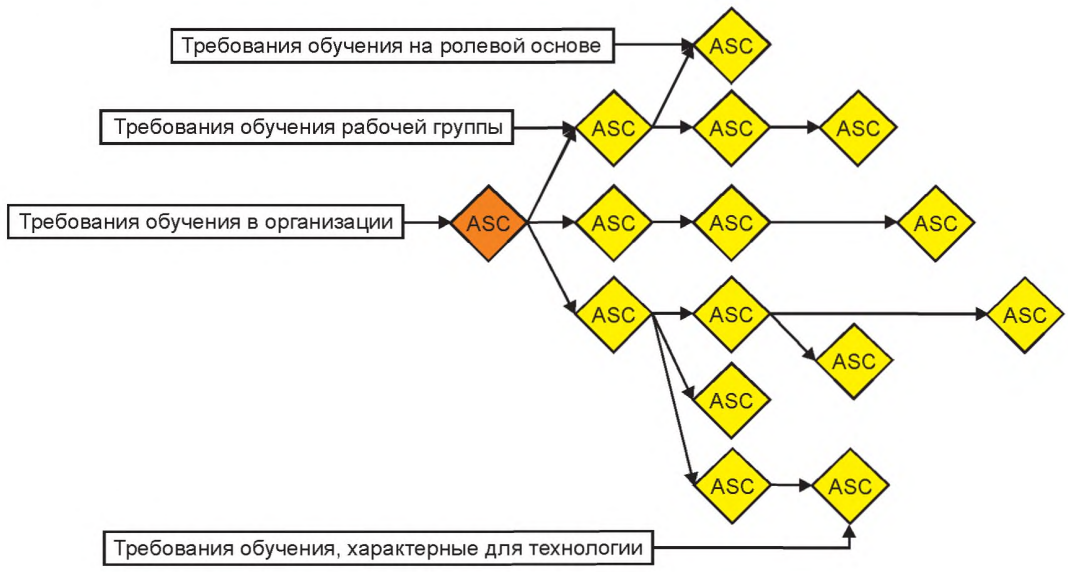

Рисунок А.3 — Пример древовидной схемы ASC

A.9.1 Обучение

1) **Требования обучения:** Все члены групп разработки программных средств должны пройти соответствующее обучение, чтобы быть в курсе основ обеспечения безопасности и последних тенденций в сфере безопасности и приватности. Лица с техническими рабочими ролями (разработчики, специалисты по тестированию, руководители программ), непосредственно участвующие в разработке программ, должны ежегодно проходить, по крайней мере, один курс обучения по безопасности. Базовое обучение по безопасности программных средств должно охватывать основополагающие концепции, такие как безопасное проектирование, моделирование угроз, определение видов атак, безопасное кодирование, тестирование безопасности и приватности.[iv]

A.9.2 Требования

2) **Требования безопасности:** Необходимость рассмотрения вопросов безопасности и приватности на базовом уровне является основополагающим аспектом разработки систем. Оптимальным моментом определения требований надежного проектирования программного средства является начальная стадия планирования его версии. Это дает возможность занимающимся разработкой группам идентифицировать ключевые этапы и результаты, а также позволяет осуществлять интеграцию безопасности и приватности таким образом, чтобы она сводила к минимуму любые нарушения планов и временны́х графиков. Анализ требований безопасности и приватности осуществляется в начале проекта и состоит из различных обязательных действий, включая (как минимум): определение применимости SDL; определение лиц, отвечающих за надзор за безопасностью и приватностью (см. 8.1.2.5 — Роли, обязанности и квалификация); определение минимальных требований безопасности; специфицирование и развертывание системы отслеживания уязвимостей/рабочих вопросов;[v]

3) **Границы качества/порог ошибок:** Границы качества/пороги ошибок используются для установления минимально допустимых уровней качества обеспечения безопасности и приватности.[vi] [vii] Определение этих критериев в самом начале проекта способствует пониманию рисков, связанных с проблемами безопасности, и дает возможность группам проекта идентифицировать и исправлять ошибки во время разработки. Группа проекта должна обсуждать границы качества для каждого этапа разработки, они должны быть утверждены куратором по безопасности с разъяснениями, соответствующими проекту, и более строгими требованиями безопасности, определенными куратором по обеспечению безопасности (в соответствующих случаях). Группа проекта должна также продемонстрировать соответствие согласованным границам качества для соблюдения требований проверки при окончательной проверке безопасности. Порог ошибок — это границы качества, относящиеся ко всему проекту разработки программных средств. Он используется для определения границ серьезности ошибок, влияющих на безопасность (например, нет *известных* ошибок в приложении с «критическим» показателем во время выпуска). Порог ошибок никогда не должен снижаться, даже если приближается дата выпуска проекта.

Примечание — Применяемая к безопасности концепция границ качества/порога ошибок близка к концепции целевого уровня доверия, так как она также используется для установления минимально допустимых уровней безопасности и приватности;

4) **Оценка риска безопасности и приватности:** Оценка риска безопасности и приватности (Security and privacy risk assessments — SRA) — это обязательные процессы идентификации функциональных аспектов программных средств, которые могут требовать углубленной проверки. Учитывая, что характеристики программы и намеченные функциональные возможности могут отличаться в разных проектах, разумно начинать с простых оценок риска и расширять их по мере необходимости для соответствия масштабу проекта. Такие оценки должны включать следующую информацию:

a) (безопасность) какие части проекта потребуют модели угроз (см. ASC 7)[1)], ниже) перед выпуском?

b) (безопасность) какие части проекта потребуют проверок проектирования безопасности перед выпуском?

c) (безопасность) какие части проекта (если таковые имеются) потребуют тестирования на проникновение, проводимого взаимно согласованной группой, являющейся внешней по отношению к группе проекта? Любые части проекта, требующие тестирования на проникновение, должны разрешить проблемы, идентифицированные во время тестирования на проникновение, перед утверждением для выпуска;

d) (безопасность) любые требования дополнительного тестирования или анализа, сочтенные куратором по обеспечению безопасности необходимыми для уменьшения рисков безопасности;

e) (безопасность) разъяснение конкретной сферы требований «случайное тестирование»[2)] (см. ASC 12)[3)], ниже);

f) (приватность) определение показателя влияния на приватность:[viii] [ix]

i) P1 — высокий риск приватности: Функция, продукт или услуга хранят или передают PII[4)] , меняют установки или ассоциации типа файла или инсталлируют программные средства;

[1)] См. перечисление 7) в A.9.3.

[2)] «Случайное тестирование» (fuzz testing) — тестирование, использующее случайный набор входных данных.

[3)] См. перечисление 12) в A.9.5.

[4)] PII (Personally Identifiable Information) — персональная идентификационная информация.

ii) P2 — средний риск приватности: Единственным влияющим на приватность видом действия в функции, продукте или услуге является однократная передача анонимных данных, инициируемая пользователем (например, пользователь щелкает по ссылке и переходит на веб-сайт);

iii) P3 — низкий риск приватности: В функции, продукте или услуге отсутствует вид действия, оказывающий влияние на приватность. Не передаются анонимные или персональные данные, не хранится в машине персональная идентификационная информация, не меняются никакие установки от имени пользователя, не инсталлируются программные средства.

А.9.3 Проектирование

5) **Требования проектирования:** Оптимальное время влияния на надежную разработку проекта — начальные моменты его жизненного цикла. Крайне важно тщательно рассматривать вопросы безопасности и приватности на этапе проектирования, так как решение проблем безопасности и приватности, осуществляемое на начальных этапах жизненного цикла, будет гораздо менее затратным. Группы проекта должны воздерживаться от практики «привязывания» к концу разработки проекта решение вопросов безопасности и приватности.

Кроме того, группам проекта крайне важно понимать различие между «безопасными свойствами» и «свойствами безопасности» — вполне возможна реализация свойств безопасности, которые, в сущности, небезопасны. Безопасные свойства определяются как свойства, функциональные возможности которых правильно спроектированы в отношении безопасности, включая строгую проверку правильности всех данных перед обработкой или криптографически надежную реализацию библиотек для криптографических сервисов. Свойства безопасности описывают функциональные возможности программы с включением безопасности (например, аутентификация по Kerberos).

Функциональные спецификации проектирования могут потребоваться для описания свойств безопасности или свойств приватности, которые будут непосредственно представлены пользователям, например, требование аутентификации пользователей для доступа к определенным данным или согласия пользователя перед использованием свойства с высоким риском приватности. В результате все спецификации проектирования должны:

a) точно и полностью определять, как реализуются эти свойства;

b) определять, как можно безопасно реализовать все функциональные возможности, разрешаемые данными свойствами;

c) определять, как безопасным способом использовать эти свойства.

Исполнение требований проектирования содержит ряд необходимых действий, включающих (но не ограничивающихся) анализ проектирования безопасности, анализ проектирования приватности и спецификаций, а также реализацию минимальных криптографических требований проектирования;[x]

6) **Уменьшение видов атак:** Уменьшение видов атак тесно связано с моделированием угроз, хотя оно рассматривает проблемы безопасности немного с иной точки зрения. Уменьшение видов атак представляет собой средство снижения риска путем предоставления нарушителям меньшей возможности для нахождения слабого места или уязвимости. Уменьшение видов атак соединяет использование многоуровневой защиты, отключение или ограничение доступа к системным сервисам и применение при любых возможных обстоятельствах принципа наименьших привилегий;

7) **Моделирование угроз:** Моделирование угроз — это обязательный процесс, выполняемый на этапе проектирования и позволяющий группам разработки в структурированном виде рассматривать, документировать и обсуждать последствия для безопасности при проектировании. Оно также предусматривает тщательное рассмотрение проблем безопасности на уровне компонентов или приложений. Моделирование угроз является командной работой, охватывающей руководителей проекта/программы, разработчиков и специалистов по тестированию, и представляет основную задачу анализа безопасности, осуществляемую на этапе проектирования программных средств.[xi]

А.9.4 Реализация

8) **Использование утвержденных инструментальных средств:** Все группы разработки должны определять и публиковать список утвержденных инструментальных средств (и конкретные функциональные возможности безопасности, такие как опции компилятора/компоновщика, предупреждающие сообщения и т. д.) для использования в программных проектах.[xii xiii] Этот список должен согласовываться и утверждаться куратором по обеспечению безопасности группы проекта. Как правило, группы разработки должны стараться использовать новейшую версию утвержденных инструментальных средств, чтобы можно было использовать новые функциональные возможности безопасности;

9) **Исключение ненадежных функций из числа используемых:** Многие обычно используемые функции и интерфейсы прикладного программирования (Application Programming Interface — API) не являются безопасными в отношении существующей среды угроз. Группы проекта должны анализировать все функции и API, которые будут использоваться совместно с проектом разработки программных средств, и запрещать те из них, которые определены как ненадежные.[xiv] После определения списка запрещенных элементов группы проекта должны использовать заголовочные файлы, обновленные компиляторы или инструментальные средства сканирования кода программы для осуществления проверки кода (включая унаследованный код в соответствующих случаях) на предмет существования запрещенных функций и замены их более надежными альтернативными вариантами;

10) **Статический анализ:** Группы проекта должны осуществлять статический анализ исходного кода программы. Статический анализ исходного кода программы обеспечивает масштабируемое решение для проверки

безопасности кода и может использоваться для обеспечения уверенности в соблюдении политик безопасного программирования, устанавливаемых руководителем группы по вопросам безопасности и куратором по обеспечению безопасности. Для проведения тщательной проверки безопасности одного статического анализа кода обычно недостаточно, отвечающая за безопасность группа и кураторы по обеспечению безопасности должны осознавать сильные и слабые стороны инструментальных средств статического анализа и быть готовыми к дополнительным задачам проверки кода другими инструментальными средствами или ручными проверками при необходимости. Облегченный статический анализ происходит во время SDL в момент регистрации кода путем использования функции */analyze* Visual Studio.[xv] Другие задачи статического анализа осуществляются по мере необходимости.

A.9.5 Верификация

11) **Динамический анализ программы:** Верификация программ во время прогона необходима для обеспечения уверенности в том, что функциональные возможности программы действуют, как было спроектировано. Динамический анализ программы должен специфицировать инструментальные средства для мониторинга поведения приложения при повреждении памяти, проблемах с привилегиями пользователей и других критических вопросах безопасности. Процесс SDL использует специальные инструментальные средства, такие как AppVerifier, а также такие методы, как «случайное» тестирование, для достижения желаемых уровней охвата тестирования безопасности;[xvi]

12) **«Случайное» тестирование:** «Случайное» тестирование используется, чтобы вызвать сбой программы путем преднамеренного введения в приложение неправильных или случайных данных. SDL определяет, что «случайное» тестирование должно проводиться на различных интерфейсах программы. Выполнение «случайных» тестов основано на намеченном использовании приложения, а также на функциональных и технических спецификациях приложения. Куратор по обеспечению безопасности может требовать дополнительного «случайного» тестирования или увеличения охвата и длительности тестирования на основе намеченного поведения приложения;[xvii]

13) **Пересмотр модели угроз/видов атак:** Существенное отклонение приложения от функциональных и технических спецификаций, созданных на этапе определения требований и создания проекта разработки программных средств, является обычной ситуацией. Поэтому важно повторное рассмотрение моделей угроз/видов атак данного приложения, когда его «код сформирован». Этот пересмотр будет обеспечивать уверенность в том, что любые изменения системы учтены, а новые векторы атак проверены и снижены;

14) **Ручная проверка кода программы (дополнительная):** Ручная проверка кода программы является дополнительной задачей в SDL. Ручная проверка кода обычно осуществляется группой, отвечающей за безопасность приложения, по рекомендации куратора по обеспечению безопасности. Хотя инструментальные средства анализа могут выполнять значительную работу по обнаружению и маркированию уязвимостей, они не совершенны, поэтому ручная проверка кода обычно сосредотачивается на «критических» компонентах приложения. Чаще всего она используется там, где затрагиваются чувствительные данные, такие как PII. Она также используется для изучения других критических компонентов, например, реализующих криптографию.

A.9.6 Выпуск

15) **План реагирования на инциденты:** Каждая версия программного продукта с учетом требований SDL должна быть охвачена планом реагирования на инциденты.[xviii] Программы, не содержащие известные уязвимости на момент выпуска, также могут подвергаться новым угрозам, возникающим с течением времени. План реагирования на инциденты должен как минимум включать следующее:

a) назначенную группу инженерной поддержки или, если группа слишком мала, чтобы обладать ресурсами инженерной поддержки, предусмотренных планом реагирования на инциденты трех — пятерых членов инженерно-технического персонала, трех — пятерых членов персонала, занимающихся маркетингом и связями с клиентами, и, по крайней мере, двух членов административного персонала, являющихся первыми контактными лицами в случае чрезвычайной ситуации, связанной с безопасностью;

b) круглосуточную телефонную связь с принимающим решения органом;

c) планы оказания услуг по безопасности для программ, предоставляемых другими группами в рамках организации;

d) планы оказания услуг по безопасности для лицензионных программ сторонних производителей — они включают имена файлов, версии, исходный код программы, контактную информацию третьей стороны и договорное разрешение на внесение изменений (в соответствующих случаях);

16) **Окончательная проверка безопасности:** Окончательная проверка безопасности (Final Security Review — FSR) — это продуманное изучение всех мероприятий по обеспечению безопасности, реализованных для прикладных программных средств до их выпуска. FSR проводится куратором по обеспечению безопасности при поддержке штатного коллектива разработчиков и руководящими лицами групп по вопросам приватности. FSR — это не проведение «проникновения и установления патчей» и не возможность проведения мероприятий по обеспечению безопасности, которые ранее игнорировались или были забыты. FSR обычно включает изучение моделей угроз, запросы исключительных ситуаций, выходные данные инструментальных средств и функционирования относительно ранее определенных границ качества/порога ошибок.[xix] FSR может приводить к одному из следующих трех результатов:

a) **FSR пройдена** — все проблемы безопасности и приватности, идентифицированные в ходе FSR, решены или уменьшены;

b) **FSR пройдена с исключительными ситуациями** — все проблемы безопасности и приватности, идентифицированные в ходе FSR, решены; те, которые не могут быть решены (например, уязвимости, представленные проблемами на уровне проектирования), фиксируются и будут исправлены в следующей версии;

c) **FSR с расширением** — если группа не выполняет все требования SDL, а куратор по обеспечению безопасности и отвечающая за продукт группа не могут достичь допустимого (или приемлемого) компромисса, то куратор по обеспечению безопасности не может утвердить проект и выпуск не может быть осуществлен. Группы должны либо решить вопросы всех возможных требований SDL до выпуска, либо обратиться к руководству для принятия решения.

Примечание — Результат FSR близок к концепции фактического уровня доверия, так как FSR — это продуманное изучение всех мероприятий по обеспечению безопасности, реализованных для прикладных программных средств до их выпуска;

17) **Выпуск/Архив:** Выпуск программного средства в производство (RTM — Read The Manual) или в вебсеть (RTW — Ready-To-Wear) обуславливает завершение процесса SDL. Назначенный куратор по обеспечению безопасности должен подтвердить, что группа проекта удовлетворила требования безопасности в отношении выпускаемого средства. Аналогичным образом для всех продуктов, имеющих, по крайней мере, один компонент с высоким риском приватности P1, куратор по обеспечению приватности должен подтвердить до отправки программного продукта, что группа проекта удовлетворила требования приватности.

Кроме того, должно быть проведено архивирование всей относящейся к делу информации и данных, чтобы после выпуска могло осуществляться обслуживание программного средства; включая все спецификации, исходный код, двоичный код, символы, модели угроз, планы реагирования на инциденты и любые другие данные, необходимые для осуществления задач по обслуживанию после выпуска.

A.10 Аудит безопасности приложений

8.5.1 Цель пятого шага ASMP состоит в верификации и формальном фиксировании подтверждающих свидетельств достижения и поддержания конкретным приложением целевого уровня доверия приложения.

Данный шаг ASMP может выполняться в любое время в течение жизненного цикла приложения. В зависимости от целевого уровня доверия приложения этот шаг может быть однократным, периодическим или обуславливаемым событиями.

Пример 1 — Организация может периодически выполнять этот шаг для мониторинга степени обеспечения безопасности на этапе реализации приложения.

Пример 2 — Организация может выполнять этот шаг для демонстрации фактического уровня доверия приложения, прежде чем будет утверждено его развертывание.

Пример 3 — Организация может выполнять этот шаг на этапе эксплуатации жизненного цикла приложения как часть ежегодно проводимого организацией аудита безопасности.

В рамках этого шага внутренняя или внешняя группа, занимающаяся верификацией (в зависимости от политик организации, содержащихся в ONF), проверяет, чтобы все верификационные измерения, представленные всеми ASC в ANF для конкретного приложения, были выполнены и результаты верифицированы. Целью данного шага является демонстрация в определенное время фактического уровня доверия приложения. Организация может объявить приложение «безопасным», когда его фактический уровень доверия равен его целевому уровню доверия.

Процесс аудита безопасности приложений для измерения фактического уровня доверия включает ряд различных действующих субъектов и процессов SDL:

- для отслеживания соответствия SDL используется специально разработанное бизнес-приложение — организовано добавление журнала инструментальных средств, моделей угроз и централизованное хранение других свидетельств, сформированных автоматически и вручную;
- руководители групп по вопросам безопасности и приватности отвечают за обеспечение уверенности в том, что все необходимые для вынесения объективного суждения данные классифицированы и введены в отслеживающее приложение;
- информация, введенная в отслеживающее приложение, затем используется кураторами по обеспечению безопасности и приватности для обеспечения структуры окончательной проверки безопасности (как описано ниже);
- кураторы по обеспечению безопасности и приватности кроме того несут ответственность за проверку данных, вводимых в отслеживающее приложение (включая результаты FSR и другие дополнительные задачи по обеспечению безопасности, установленные куратором), и подтверждение того, что все требования выполнены и/или вопросы всех несоответствий разрешены.

На рисунке А.4 показан снимок экрана приложения, используемого для отслеживания и верификации задач по обеспечению безопасности.

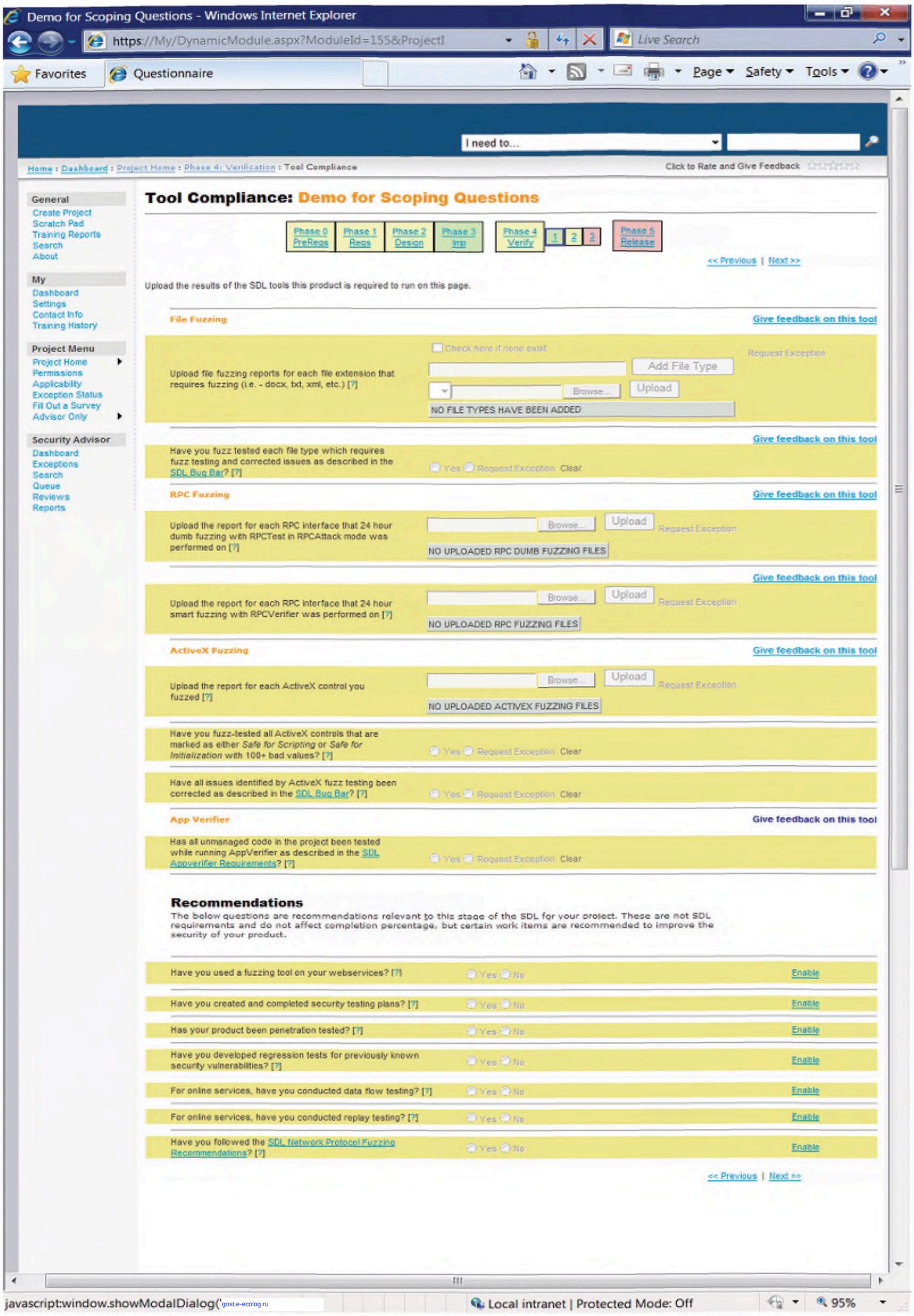

Рисунок А.4 — Пример применения бизнес-приложения для аудита безопасности приложений

А.11 Модель жизненного цикла приложений

8.1.2.7.1 Организация, бизнес которой включает разработку, аутсорсинг или приобретение приложений, обычно использует структуру определенных процессов или деятельности, систематизированную по этапам. Эта структура обычно называется «моделью жизненного цикла». Но в зависимости от контекста ее еще называют «моделью жизненного цикла приложений», либо «моделью жизненного цикла систем», либо «моделью жизненного цикла программных средств».

Такая модель обычно уникальна для конкретной организации и приспособлена к ее требованиям. Она используется и совершенствуется в течение многих лет. Это не новое понятие, введенное ИСО/МЭК 27034.

Жизненный цикл определенного приложения, т. е. развитие приложения от замысла до снятия с эксплуатации, представляет собой конкретизацию модели жизненного цикла организации.

В организациях со сложной структурой различные группы, возможно, будут использовать разные модели жизненного цикла приложений для разных проектов. Так часто происходит в крупных децентрализованных организациях или организациях, сформированных путем слияния. В других организациях будут разрабатываться различные специализированные модели жизненного цикла приложений, относящиеся к определенному контексту приложений, например, веб-приложения, приложения, работающие в режиме реального времени, встроенные приложения, медицинские приложения и т. д.

В данном случае исследование модели жизненного цикла приложений используется для составления мероприятий безопасности SDL. В предыдущих разделах данного документа описываются бизнес-контекст, технический и регулятивный контексты и роли, действующие в каждой из этих сфер.

Иллюстрация процесса SDL представлена на рисунке А.5. Эта схема является визуализацией мер и средств контроля и управления безопасностью приложений, используемых в гипотетическом проекте — от обучения служащих до выпуска приложений. Эта схема не является исчерпывающей; как отмечалось ранее, многие группы добавляют характерные для их проектов задачи обеспечения безопасности и приватности.

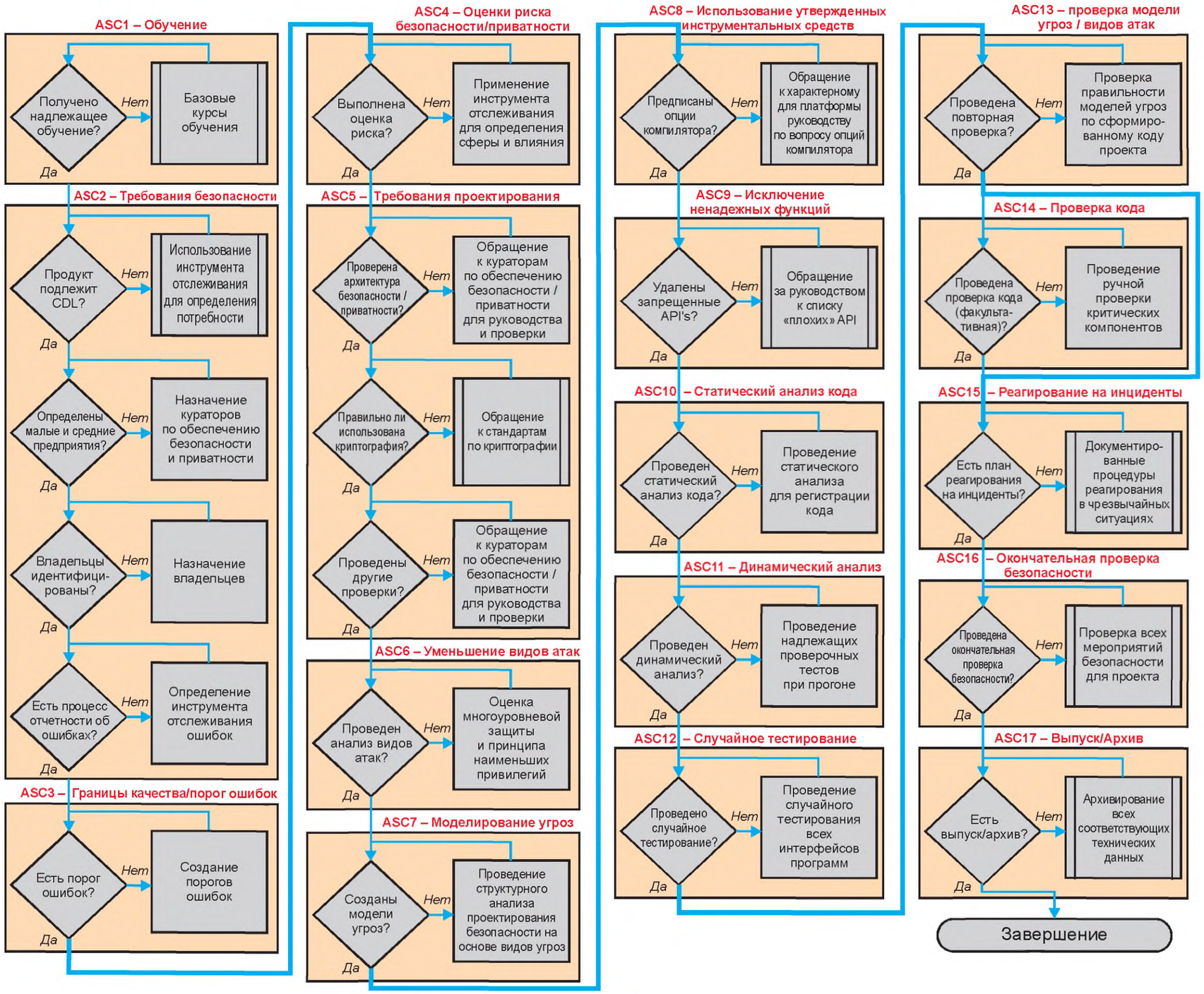

Рисунок А.5 — Иллюстрация процесса SDL

А.12 Сопоставление SDL с эталонной моделью жизненного цикла безопасности приложений

Процесс SDL можно сопоставить с включенной в ИСО/МЭК 27034 схемой эталонной модели жизненного цикла безопасности приложений. Этапы эталонной модели, охватываемые процессом SDL, на рисунке А.6 выделены полужирным шрифтом.



Рисунок А.6 — Сопоставление SDL с эталонной моделью жизненного цикла безопасности приложений

На рисунке А.7 показано более детальное сопоставление этапов SDL с этапами эталонной модели жизненного цикла безопасности приложений.

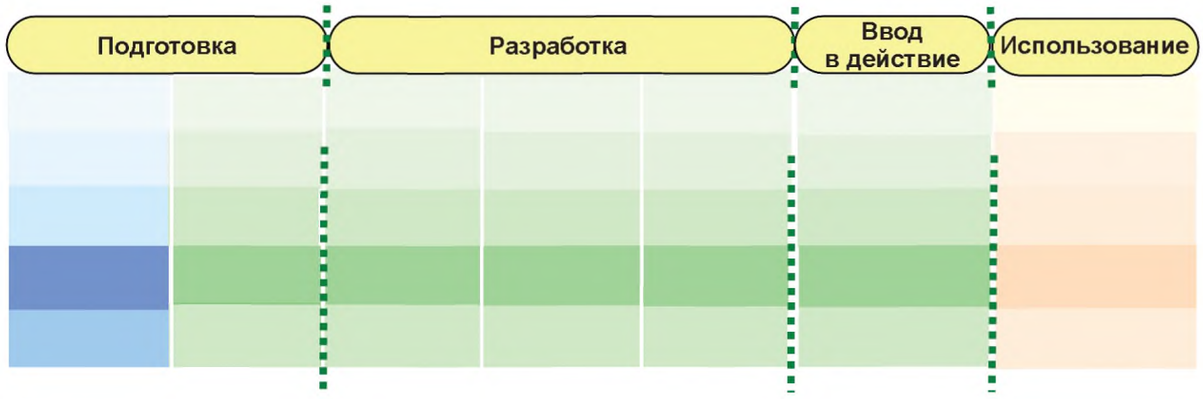

Рисунок А.7 — Детальное сопоставление этапов SDL с этапами эталонной модели жизненного цикла безопасности приложений

Ссылки в Приложении А

Бизнес-контекст

i gost.e-ecolog.ru

ii gost.e-ecolog.ru

Роли, обязанности и квалификация

iii gost.e-ecolog.ru

Библиотека ASC организации

Обучение

iv gost.e-ecolog.ru

Требования

v gost.e-ecolog.ru

vi gost.e-ecolog.ru (Безопасность)

vii gost.e-ecolog.ru (Приватность)

viii gost.e-ecolog.ru

ix gost.e-ecolog.ru

gost.e-ecolog.ru

Проектирование

x gost.e-ecolog.ru

xi gost.e-ecolog.ru

Реализация

xii gost.e-ecolog.ru

xiii gost.e-ecolog.ru

xiv gost.e-ecolog.ru

xv gost.e-ecolog.ru

xvi gost.e-ecolog.ru

xvii gost.e-ecolog.ru

xviii gost.e-ecolog.ru

xix gost.e-ecolog.ru

Приложение В
(справочное)

Сопоставление ASC существующих стандартов

Пример: сопоставление мер и средств контроля и управления безопасностью приложений, описанных в NIST SP 800-53 (редакция 3), с ASC, описанными в ИСО/МЭК 27034

Цель данного приложения — проиллюстрировать, как меры и средства контроля и управления безопасностью приложений из существующего источника, например из третьей редакции NIST SP 800-53, могут быть интегрированы как ASC для использования в соответствии с ИСО/МЭК 27034.

В.1 Категории потенциальных ASC

В данном подразделе сделана попытка рассмотреть возможные аспекты категорий потенциальных ASC, непосредственно приводимых в SP 800-53 (редакция 3).

Организация может определить следующие аспекты категории ASC, связанные с безопасностью приложений.

В.1.1 Аспекты, связанные с общими мерами и средствами контроля и управления безопасностью

Менеджмент мер и средств контроля и управления безопасностью, обозначенных организацией как общие меры и средства контроля и управления, в большинстве случаев осуществляется организационной сущностью, отличной от владельца информационной системы. Организационные решения, касающиеся общих мер и средств контроля и управления безопасностью, могут существенно повлиять на обязанности отдельных собственников информационной системы в связи с реализацией мер и средств контроля и управления в соответствии с тем или иным базовым уровнем. Каждая мера и средство контроля и управления на базовом уровне должны полностью рассматриваться либо организацией, либо владельцем информационной системы.

В.1.2 Аспекты, связанные с операционной деятельностью/средой

Меры и средства контроля и управления безопасностью, зависящие от характера операционной среды, применимы только в том случае, если информационная система используется в условиях, требующих этих мер и средств контроля и управления. Например, определенные меры и средства контроля и управления физической безопасностью могут быть неприменимы для космических информационных систем, а меры и средства контроля и управления температурой и влажностью могут быть неприменимы для дистанционных датчиков, существующих вне помещений, которые содержат информационные системы.

В.1.3 Аспекты, связанные с физической инфраструктурой

Меры и средства контроля и управления безопасностью, относящиеся к физической инфраструктуре, например к помещениям организации (физические меры и средства контроля и управления, такие как замки и охрана, меры и средства контроля и управления защитой от влияния внешней среды: температуры, влажности, грозовых разрядов, возгорания и проблем энергоснабжения), применимы только к тем их частям, которые непосредственно обеспечивают защиту и поддержку информационных систем или связаны с информационными системами (включая активы информационных технологий, такие как почтовые и веб-серверы, группы серверов, информационные центры, сетевые узлы, устройства защиты границ и аппаратура связи).

В.1.4 Аспекты, связанные с открытым доступом

Меры и средства контроля и управления безопасностью, связанные с общедоступными информационными системами, должны тщательно рассматриваться и применяться с осторожностью, поскольку некоторые меры и средства контроля и управления безопасностью определенных базовых уровней контроля и управления (например, идентификация и аутентификация, управление безопасностью персонала) могут быть неприменимы для пользователей, получающих доступ к информационным системам через общедоступные интерфейсы. Например, наряду с тем, что меры и средства контроля и управления безопасностью базового уровня требуют идентификации и аутентификации персонала организации, осуществляющего техническое обслуживание и поддержку информационных систем, предоставляющих услуги открытого доступа, те же меры и средства контроля и управления безопасностью могут не потребоваться для доступа к информационным системам через общедоступные интерфейсы для получения общедоступной информации. С другой стороны, в некоторых случаях будет требоваться идентификация и аутентификация для пользователей, получающих доступ к информационным системам через общедоступные интерфейсы, например, для доступа/изменения своей персональной информации.

В.1.5 Аспекты, связанные с технологией

Меры и средства контроля и управления безопасностью, относящиеся к определенным технологиям (например, беспроводная связь, криптография, инфраструктура открытых ключей), применимы только в том случае, если эти технологии используются в информационной системе или требуется их использование.

Меры и средства контроля и управления безопасностью применимы только к компонентам информационной системы, обеспечивающим или поддерживающим возможности безопасности, на которые направлены меры и средства контроля и управления безопасностью, и являющимися источниками потенциального риска, уменьшае-

мого посредством мер и средств контроля и управления безопасностью. Например, если компоненты информационной системы являются однопользовательскими, а не относящимися к сетевой структуре или локальной сетевой структуре, то одна или несколько таких характеристик могут обеспечивать соответствующее логическое обоснование для неприменения выбранных мер и средств контроля и управления безопасностью к данному компоненту.

Меры и средства контроля и управления безопасностью, которые могут явно или неявно поддерживаться автоматическими механизмами, не требуют разработки таких механизмов, если они еще не существуют или недоступны среди продуктов, готовых к использованию в коммерческих или государственных целях. В ситуациях, когда автоматические механизмы не являются доступными, экономически эффективными или технически осуществимыми, для компенсации определенных мер и средств контроля и управления безопасностью или расширений мер и средств контроля и управления, необходимо использовать компенсационные меры и средства контроля и управления безопасностью, реализующиеся путем неавтоматизированных механизмов или процедур (условия применения компенсационных мер и средств контроля и управления см. ниже).

B.1.6 Аспекты, связанные с политикой/регулятивными требованиями

Меры и средства контроля и управления безопасностью, предназначенные для решения вопросов, регулируемых соответствующими законами, административными указами, директивами, политиками, стандартами или предписаниями (например, оценки влияния на приватность), требуются только в том случае, если применение этих мер и средств контроля и управления безопасностью согласуется с видами информации и информационных систем, охватываемых соответствующими законами, административными указами, директивами, политиками, стандартами или предписаниями.

B.1.7 Аспекты, связанные с масштабируемостью

Меры и средства контроля и управления безопасностью масштабируемы в отношении объема и строгости реализации контроля и управления. Масштабируемость регулируется классификацией безопасности защищаемой информационной системы по FIPS 199. Например, план действий в чрезвычайных ситуациях для информационной системы с высоким влиянием по FIPS 199 может быть весьма объемным и содержать значительное количество деталей реализации. В отличие от этого план действий в чрезвычайных ситуациях для информационной системы с низким влиянием по FIPS 199 может быть значительно короче и содержать гораздо меньше деталей реализации. Организации должны осмотрительно применять меры и средства контроля и управления безопасностью к информационным системам, учитывая факторы масштабируемости в конкретной среде. Такой подход способствует экономически эффективному, основанному на риске подходу к реализации мер и средств контроля и управления безопасностью, при котором затрачивается ресурсов не больше, чем это необходимо, однако достигаются существенное уменьшение риска и адекватная безопасность.

B.1.8 Аспекты, связанные с целями безопасности

Меры и средства контроля и управления безопасностью, однозначным образом поддерживающие цели безопасности по обеспечению конфиденциальности, целостности или доступности, могут быть понижены до более низкого базового уровня мер и средств контроля и управления (соответствующим образом модифицированы или устранены, если они не определены в более низком базовом уровне) тогда и только тогда, если такое понижение: (i) согласуется с классификацией безопасности FIPS 199 для соответствующих целей безопасности по обеспечению конфиденциальности, целостности или доступности до перемещения на отметку максимального уровня; (ii) поддерживается оценкой риска организации; (iii) не влияет на имеющую отношение к безопасности информацию в информационной системе. Рекомендуемыми на понижение мерами и средствами контроля и управления безопасностью являются следующие: (i) конфиденциальность [AC-15, MA-3 (3), MP-2 (1), MP-3, MP-4, MP-5 (1) (2) (3), MP-6, PE-5, SC-4, SC-9]; (ii) целостность [SC-8] и (iii) доступность [CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, MA-6, PE-9, PE-10, PE-11, PE-13, PE-15, SC-6].

B.2 Классы мер и средств контроля и управления безопасностью

В данном подразделе представлена классификации ASC, взятых из SP 800-53 (редакция 3).

Таблица B.1 — Идентификаторы, семейства и классы мер и средств контроля и управления безопасностью

Идентификатор	Семейство	Класс
AC	Управление доступом	Технические
AT	Информирование и обучение	Операционные
AU	Аудит и подотчетность	Технические
CA	Сертификация, аккредитация и оценки безопасности	Административные
CM	Менеджмент конфигурации	Операционные
CP	Планирование действий в чрезвычайных ситуациях	Операционные
IA	Идентификация и аутентификация	Технические

Окончание таблицы В.1

Идентификатор	Семейство	Класс
IR	Реагирование на инциденты	Операционные
MA	Техническое обслуживание	Операционные
MP	Защита носителей данных	Операционные
PE	Физическая защита и защита от влияния внешней среды	Операционные
PL	Планирование	Административные
PS	Безопасность, связанная с персоналом	Операционные
RA	Оценка риска	Административные
SA	Приобретение систем и услуг	Административные
SC	Защита систем и средств связи	Технические
SI	Целостность информации и систем	Операционные

В.3 Подклассы класса мер и средств контроля и управления доступом (AC)

В данном подразделе рассматривается взятая непосредственно из SP 800-53 (редакция 3) информация, которая может быть использована для создания мер и средств контроля и управления безопасностью приложений, связанных с управлением доступом.

Таблица В.2 — Классы мер и средств контроля и управления безопасностью и базовые уровни контроля и управления безопасностью для информационных систем с низким, средним и высоким уровнем влияния

Название меры и средства контроля и управления безопасностью		Уровень контроля		
Управление доступом		Низкий	Средний	Высокий
AC-1	Политика и процедуры управления доступом	AC-1	AC-1	
AC-2	Менеджмент учетных записей	AC-2	AC-2 (1) (2) (3) (4)	AC-2 (1) (2) (3) (4)
AC-3	Обеспечение доступа	AC-3	AC-3 (1)	AC-3 (1)
AC-4	Обеспечение информационного потока	Не выбран	AC-4	AC-4
AC-5	Разделение обязанностей	Не выбран	AC-5	AC-5
AC-6	Принцип наименьших привилегий	Не выбран	AC-6	AC-6
AC-7	Неуспешные попытки регистрации	AC-7	AC-7	AC-7
AC-8	Уведомление об использовании системы	AC-8	AC-8	AC-8
AC-9	Уведомление о предыдущем входе в систему	Не выбран	Не выбран	Не выбран
AC-10	Контроль одновременных сессий	Не выбран	Не выбран	AC-10
AC-11	Блокирование сессии	Не выбран	AC-11	AC-11
AC-12	Завершение сессии	Не выбран	AC-12	AC-12 (1)
AC-13	Надзор и проверка — управление доступом	AC-13	AC-13 (1)	AC-13 (1)
AC-14	Разрешенные действия без идентификации и аутентификации	AC-14	AC-14 (1)	AC-14 (1)
AC-15	Автоматическая маркировка	Не выбран	Не выбран	AC-15
AC-16	Автоматическое присваивание меток	Не выбран	Не выбран	Не выбран
AC-17	Удаленный доступ	AC-17	AC-17 (1) (2) (3) (4)	AC-17 (1) (2) (3) (4)

Окончание таблицы В.2

Название меры и средства контроля и управления безопасностью		Уровень контроля		
Управление доступом		Низкий	Средний	Высокий
AC-18	Ограничения беспроводного доступа	AC-18	AC-18 (1)	AC-18 (1) (2)
AC-19	Управление доступом для портативных и мобильных устройств	Не выбран	AC-19	AC-19
AC-20	Использование внешних информационных систем	AC-20	AC-20 (1)	AC-20 (1)

В.4 Детализация класса мер и средств контроля и управления доступом

В данном подразделе показаны три семейства класса управления доступом: AC-1, AC-2, AC-17, которые взяты из SP 800-53 (редакция 3).

СЕМЕЙСТВО: УПРАВЛЕНИЕ ДОСТУПОМ **КЛАСС:** ТЕХНИЧЕСКИЕ

В.4.1 AC-1 Политика и процедуры управления доступом

Мера и средство контроля и управления: Организация разрабатывает, распространяет и периодически пересматривает/обновляет:

1) надлежащим образом документально оформленную политику управления доступом, рассматривающую цели, сферу действия, роли, обязанности, обязательства руководства, координацию организационных подразделений и соответствие требованиям;

2) надлежащим образом документально оформленные процедуры для содействия реализации политики управления доступом и соответствующих мер и средств контроля и управления доступом.

Дополнительное руководство: Политика и процедуры управления доступом согласуются с применяемыми законами, распоряжениями правительства, директивами, политиками, предписаниями, стандартами и руководствами. Политика управления доступом может включаться в общую политику информационной безопасности организации как отдельная часть. Процедуры управления доступом могут разрабатываться для программы обеспечения безопасности в целом и, когда необходимо, для конкретной информационной системы. Специальная публикация NIST SP 800-12 предоставляет руководство по политикам и процедурам обеспечения безопасности.

Приоритетность и базовое размещение:

Расширения мер и средств контроля и управления: Нет. Низкий AC-1	Средний AC-1	Высокий AC-1

В.4.2 AC-2 Менеджмент учетных записей

Мера и средство контроля и управления: Организация осуществляет менеджмент учетных записей информационной системы, включая:

1) идентификацию типов учетных записей (например, индивидуальные, групповые и системные);

2) установление условий для членства в группе;

3) идентификацию уполномоченных пользователей информационной системы и определение прав/привилегий доступа;

4) требование соответствующего утверждения запросов о создании учетных записей;

5) санкционирование, создание, активацию, модификацию, блокирование и удаление учетных записей;

6) проверку учетных записей [Назначение: устанавливаемая организацией частота];

7) специальное санкционирование и мониторинг использования гостевых/анонимных учетных записей;

8) уведомление лиц, осуществляющих менеджмент учетных записей, об увольнении и переводе пользователей информационной системы или об изменении использования информационной системы или принципа необходимого знания/необходимого совместного использования;

9) предоставление доступа к информационной системе на основе: (i) принципа необходимого знания или необходимого совместного использования, который определяется назначенными должностными обязанностями и соответствием всем критериям безопасности, связанным с персоналом; (ii) предназначенного использования системы.

Дополнительное руководство: Идентификация уполномоченных пользователей информационной системы и определение прав/привилегий доступа согласуются с требованиями других мер и средств контроля и управления безопасностью в плане обеспечения безопасности. Взаимосвязанные меры и средства контроля и управления: AC-1, AC-3, AC-4, AC-5, AC-6, AC-10, AC-13, AC-17, AC-19, AC-20, AU-9, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SI-9, SC-13.

Расширения меры и средства контроля и управления:

1) организация использует механизмы автоматизации для поддержки менеджмента учетных записей информационной системы;

2) информационная система автоматически прекращает действие врéменных учетных записей и учетных записей об аварийных ситуациях после [Назначение: устанавливаемый организацией период времени для каждого вида учетных записей];

3) информационная система автоматически блокирует неактивные учетные записи после [Назначение: устанавливаемый организацией период времени];

4) информационная система автоматически осуществляет аудит создания, модификации, блокирования и прекращения действия учетных записей и уведомляет по требованию соответствующих лиц;

5) организация проводит проверку активных на настоящий момент учетных записей информационной системы [Назначение: устанавливаемая организацией частота] для подтверждения того, что врéменные учетные записи и учетные записи уволившихся или переведенных пользователей деактивированы в соответствии с политикой организации;

6) организация запрещает использование идентификаторов учетных записей информационной системы в качестве идентификаторов учетных записей электронной почты.

Приоритетность и базовое размещение:

Низкий AC-2	Средний AC-2 (1) (2) (3) (4) (5) (6)	Высокий AC-2 (1) (2) (3) (4) (5) (6)

B.4.3 AC-17 Удаленный доступ

Мера и средство контроля и управления: Организация:

1) документирует разрешенные методы удаленного доступа к информационной системе;

2) устанавливает ограничения на использование и руководство по реализации для каждого разрешенного метода удаленного доступа;

3) санкционирует удаленный доступ к информационной системе до подключения;

4) обеспечивает соблюдение требований удаленного подключения к информационной системе.

Дополнительное руководство: Удаленным доступом является любой доступ пользователя (или процесса, действующего от имени пользователя) к информационной системе организации по внешней, не контролируемой организацией сети (например, Интернет). Примеры методов удаленного доступа: коммутируемое соединение по телефонной линии, широкополосный доступ и беспроводной доступ. Виртуальная частная сеть (Virtual Private Network — VPN) при адекватном обеспечении может рассматриваться как контролируемая организацией сеть. При беспроводном доступе излучаемые сигналы в пределах контролируемых организацией помещений обычно рассматриваются как находящиеся вне контроля организации. Беспроводные технологии включают (но не ограничиваются) СВЧ-связь, спутниковую связь, пакетную радиосвязь (УВЧ/ОВЧ), 802.11x и Bluetooth. Меры и средства контроля и управления удаленным доступом применимы к информационным системам, отличным от общедоступных вебсерверов или систем, специально предназначенных для открытого доступа. Обеспечение соблюдения связанных с удаленными соединениями ограничений доступа к информационной системе осуществляется посредством меры и средства контроля и управления AC-3. NIST SP 800-77 предоставляет руководство по виртуальным частным сетям на основе протокола IPsec, NIST SP 800-48 и NIST SP 800-97 — руководство по безопасности беспроводной сети, NIST SP 800-94 — руководство по обнаружению и предотвращению беспроводного вторжения. Взаимосвязанные меры и средства контроля и управления: AC-1, AC-3, AC-20, IA-2, IA-8.

Расширения меры и средства контроля и управления:

1) организация использует механизмы автоматизации для облегчения мониторинга и контроля методов удаленного доступа;

2) организация использует криптографию для защиты конфиденциальности и целостности сеансов связи удаленного доступа.

Дополнительное руководство по расширению: Стойкость криптографического механизма выбирается на основе уровня влияния на информацию по FIPS 199. Взаимосвязанные меры и средства контроля и управления: SC-8, SC-9;

3) информационная система направляет весь удаленный доступ через ограниченное число контролируемых точек управления доступом;

4) организация санкционирует удаленный доступ к привилегированным командам и относящейся к безопасности информации только при настоятельной операционной потребности и документирует логическое обоснование такого доступа в плане обеспечения безопасности для информационной системы.

Дополнительное руководство по расширению: Взаимосвязанная мера и средство контроля и управления: AC-6;

5) информационная система обеспечивает защиту беспроводного доступа к системе, используя аутентификацию и шифрование.

Дополнительное руководство по расширению: Аутентификация применяется к пользователям, устройствам или и к тем и другим, при необходимости;

6) организация осуществляет мониторинг на предмет несанкционированных удаленных соединений с информационной системой, включая сканирование на предмет несанкционированных точек беспроводного доступа [*Назначение: устанавливаемая организацией частота*], и принимает соответствующие меры при обнаружении несанкционированного соединения.

Дополнительное руководство по расширению: Организации осуществляют профилактический поиск несанкционированных удаленных соединений, включая проведение тщательного сканирования на предмет несанкционированных точек беспроводного доступа. Сканирование необязательно ограничено только теми областями в объекте, которые содержат информационные системы, однако за пределами этих областей оно проводится только при необходимости подтверждения того, что несанкционированные точки беспроводного доступа не соединены с системой;

7) организация отключает не планируемые для использования беспроводные сетевые возможности, которые внутренне встроены в компоненты информационной системы, до выпуска;

8) организация не разрешает пользователям самостоятельно конфигурировать беспроводные сетевые возможности;

9) организация обеспечивает уверенность в том, что пользователи защищают информацию о механизмах удаленного доступа от несанкционированного использования и раскрытия;

10) организация обеспечивает уверенность в том, что удаленные сеансы связи для доступа к [*Назначение: устанавливаемый организацией список функций безопасности и информации, относящейся к безопасности*] используют дополнительные меры безопасности [*Назначение: устанавливаемые организацией меры безопасности*] и подвергаются аудиту;

11) организация отключает беспроводные одноранговые сетевые возможности в информационной системе, за исключением однозначно идентифицируемых компонентов, в поддержку конкретных операционных требований;

12) организация отключает беспроводные сетевые возможности Bluetooth в информационной системе, за исключением однозначно идентифицируемых компонентов, в поддержку конкретных операционных требований.

Приоритетность и базовое размещение:

Низкий AC-17	Средний AC-17 (1) (2) (3) (4) (5)	Высокий AC-17 (1) (2) (3) (4) (5) (6)

B.5 Описание ASC, основанное на примере мер и средств контроля и управления из SP 800-53

В данном подразделе представлено, как мера и средство контроля и управления AU-14 из SP 800-53 (редакция 3) может быть описана с использованием структуры мер и средств контроля и управления безопасностью приложений ИСО/МЭК 27034.

Полная и точная структура данных мер и средств контроля и управления безопасностью приложений будет представлена в ИСО/МЭК 27034-5.

B.5.1 Мера и средство контроля и управления AU-14, описанная в SP 800-53 (редакция 3)

Мера и средство контроля и управления AU-14 описывается в SP 800-53 (редакция 3) следующим образом:

AU-14 АУДИТ СЕАНСА СВЯЗИ

Мера и средство контроля и управления: Информационная система предоставляет возможность:

a) сбора/регистрации и протоколирования всего контента, связанного с сеансом связи пользователя;

b) удаленного просмотра/прослушивания всего контента, связанного с установленным сеансом связи пользователя, в режиме реального времени.

Дополнительное руководство: Мероприятия аудита сеанса связи разрабатываются, интегрируются и используются после консультации с юрисконсультом в соответствии с применяемыми федеральными законами, административными указами, директивами, политиками или предписаниями.

Расширения меры и средства контроля и управления:

1) информационная система инициирует аудиты сеансов связи при запуске системы.

Ссылки: Нет.

Приоритетность и базовое размещение:

Низкий Не выбран	Средний Не выбран	Высокий Не выбран

B.5.2 Мера и средство контроля и управления AU-14, описанная с использованием формата ASC ИСО/МЭК 27034

Мера и средство контроля и управления AU-14 может быть описана как ASC в соответствии с ИСО/МЭК 27034, как показано в таблице B.3.

Таблица В.3 — Мера и средство контроля и управления AU-14 из SP 800-53, описанная с использованием формата ASC ИСО/МЭК 27034

Поле	Описание	Значение
Идентификация ASC:		
ASC-AU-14_Id-Label:	Текст: Название ASC	Аудит сеанса связи
ASC-AU-14_Id-UID:	Текст: Уникальный идентификационный номер ASC	ASC-AU-14
ASC-AU-14_Id-Description:	Текст: Описание ASC открытым текстом	Информационная система предоставляет возможность: a) сбора/регистрации и протоколирования всего контента, связанного с сеансом связи пользователя; b) удаленного просмотра/прослушивания всего контента, связанного с установленным сеансом связи пользователя, в режиме реального времени. Дополнительное руководство: Мероприятия аудита сеанса связи разрабатываются, интегрируются и используются после консультации с юрисконсультом в соответствии с применяемыми федеральными законами, административными указами, директивами, политиками или предписаниями
ASC-AU-14_Id-Author name	Текст: фамилия, имя, отчество	Wubu, Daming
ASC-AU-14_Id-Author company name	Текст:	Корпорация ACME
ASC-AU-14_Id-Author email	Текст: адрес электронной почты	gost.e-ecolog.ru
ASC-AU-14_Id-Author signature	Знаковая хэш-функция исходной ASC	894735897073420527906724 8
ASC-AU-14_Id-Organization UID:	Идентификатор (ID) организации	JTC1/SC27 WG4 27034-1 WD3 01-001
ASC-AU-14_Id-Creation date:	Дата: год-месяц-день	2009-04-08
ASC-AU-14_Id-Pointer to parent:	Материнская ASC: Список ID ASC или Нулевая информация	Нулевая информация
ASC-AU-14_Id-Pointer to children:	Дочерняя ASC: Список ID ASC или Нулевая информация	Нулевая информация
ASC-AU-14_Id-Pointers to the business context:	Список бизнес-контекста или Нулевая информация	Финансовая
ASC-AU-14_Id-Pointer to the regulatory context:	Список регулятивного контекста или Нулевая информация	Закон об обеспечении приватности #RF76G7, статья 4.11
ASC-AU-14_Id-Pointer to the technological context:	Список технологического контекста или Нулевая информация	Нулевая информация
ASC-AU-14_App_Specification:	Спецификации приложения, обеспечивающие требования безопасности для ASC	Приложение устанавливает стабильный сеанс связи

Продолжение таблицы В.3

Поле	Описание	Значение
ASC-AU-14_Id-ASC XML version	Версия XML-схемы ASC: Номер версии	v1.0 Beta
Цели ASC:		
ASC-AU-14_Obj-Level-of-Trust:	1 или n — целевые уровни доверия: на каком уровне доверия активна данная ASC. Может быть связана с несколькими уровнями	5, 6, 7, 8, 9
ASC-AU-14_Obj-why:	Причины существования данной ASC. Идентификация потребностей руководства, руководителя группы, группы разработки, аудитора и т. д. Цель также точно определяет, что будет оцениваться	Обеспечение уверенности в том, что пользователь соблюдает закон об обеспечении приватности #RF76G7, статья 4.11, и политику организации по допустимому использованию
ASC-AU-14_LevelOfTrust-TotalLevels:	Диапазон уровней доверия, используемый организацией	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
ASC-AU-14_LevelOfTrust-why:		Аудит сеанса связи требует значительных ресурсов и необходим только для приложений, обрабатывающих персональную информацию
ASC-AU-14_AppSpec_ComplToReg_St ds&BestPractices:	Стандарты, с которыми связана данная ASC (ITIL, Cobit, ИСО 17799, RUP, название образца проектирования и т. д.)	NIST SP-800-53 Rev. 3, AU-14
Мероприятие по обеспечению безопасности ASC:		
ASC-AU-14_SecAct-Label:	Текст: Название мероприятия	Реализация класса аудита сеанса связи из утвержденной библиотеки по безопасности
ASC-AU-14_SecAct-UID:	Текст: Уникальный ID мероприятия обеспечения безопасности	ACT-001-JAVA027
ASC-AU-14_SecAct-Description:	Полное описание мероприятия. Оно представляет, кто что выполняет. Ориентировочно, это описание процессов и действующих субъектов, необходимых для реализации или оценивания меры	Использование утвержденной организацией библиотеки по безопасности JAVA для реализации безопасного процесса аудита сеанса связи в приложении
ASC-AU-14_SecAct-Complexity:	Сложность мероприятия: Простое, стандартное, сложное, очень сложное	Простое
ASC-AU-14_SecAct-who_Role:	Существующая роль в организации	Разработчик
ASC-AU-14_SecAct-who_Responsibility:	R = реализация, P = участие, ...	R
ASC-AU-14_SecAct-who_Qualification:	Квалификация для мероприятия: Представляет необходимую квалификацию действующих субъектов	Средний или более высокий уровень квалификации разработчика

Окончание таблицы В.3

Поле	Описание	Значение
ASC-AU-14_SecAct-When:	Целевая точка мероприятия в эталонной модели жизненного цикла безопасности приложений ИСО/МЭК 27034	Этап разработки, мероприятие разработки элементов
ASC-AU-14_SecAct-Artefact:	Артефакт: Название и описание артефакта, создаваемого в результате мероприятия	Обращение к соответствующему примеру JAVA
ASC-AU-14_SecAct-Result_Expected:	Ожидаемые результаты: Описание ситуации, состояния или точного значения артефакта	Для каждой транзакции класс обязан посылать детали транзакций в службу безопасного протоколирования организации. В конце этого мероприятия ожидаются результаты тестирования элементов и документация стратегии
ASC-AU-14_SecAct-cost:	Стоимость мероприятия: Стоимость выполнения этого мероприятия (человеко-дни, денежные суммы и т. д.)	10 человеко-дней
Верификационное измерение ASC:		
ASC-AU-14_VerfMeas-Label:		Верификация реализации компонентов аудита сеанса связи
ASC-AU-14_VerfMeas-UID:		VeM-001-JAVA453
ASC-AU-14_VerfMeas-Description:		Верификация того, что для каждой транзакции класс посылает детали транзакций в службу безопасного протоколирования организации. Верификация того, что результаты тестирования элементов и документация стратегии представлены и являются успешными
ASC-AU-14_VerfMeas-Complexity	Сложность верификационного измерения: Простое, стандартное, сложное, очень сложное	Стандартное
ASC-AU-14_VerfMeas-who_Role:		Главный специалист по проверке кода
ASC-AU-14_VerfMeas-who_Responsability:	R = реализация, P = участие, …	R
ASC-AU-14_VerfMeas-who_Qualification:	Квалификация для мероприятия контроля: Представляет необходимую квалификацию действующих субъектов	Старший разработчик Java
ASC-AU-14_VerfMeas-when_Phase:	Целевая деятельность в эталонной модели жизненного цикла безопасности приложений ИСО/МЭК 27034	Этап разработки, мероприятие функционального тестирования
ASC-AU-14_VerfMeas-Artefact:		Результат должен быть TRUE для всех верификационных измерений
ASC-AU-14_VerfMeas-cost:	Затраты на контрольные мероприятия: Затраты на верификацию этого мероприятия (человеко-дни, денежные суммы и т. д.). Может определять потребность в периодической оценке	1 человеко-день

Приложение С
(справочное)

Сопоставление процесса менеджмента риска из ИСО/МЭК 27005 с ASMP

ASMP можно рассматривать с точки зрения менеджмента риска, следуя, таким образом, процессу, подобному процессу менеджмента риска, определенному в ИСО/МЭК 27005.

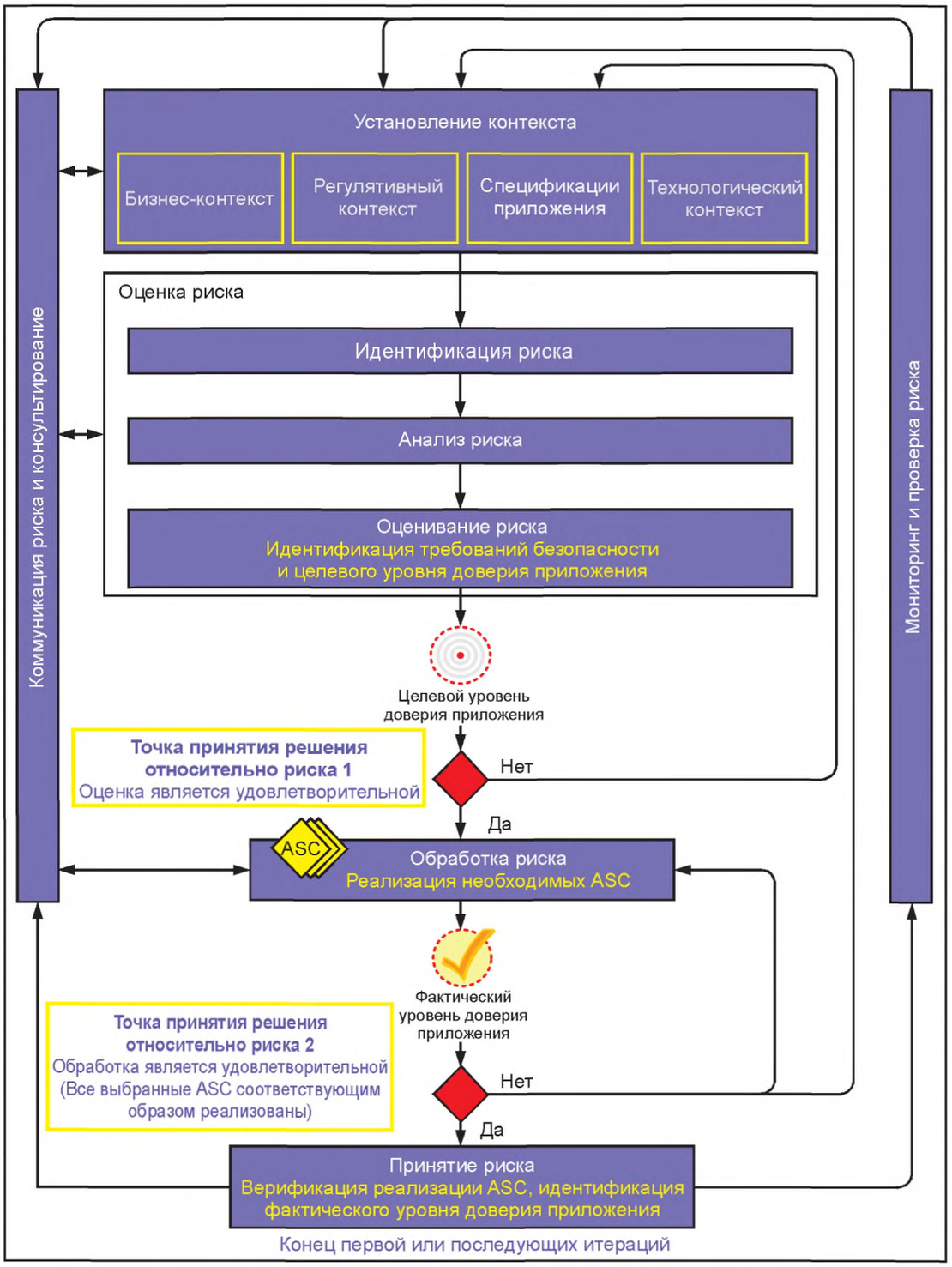

Рисунок С.1 — Сопоставление процесса менеджмента риска из ИСО/МЭК 27005 с процессом ASMP

Выполняются следующие элементы процесса. Сначала устанавливается контекст приложения. Затем проводится оценка риска на уровне приложений. Если это предоставляет достаточно информации для эффективного определения мер и средств контроля и управления, которые необходимы для уменьшения рисков из-за использования организацией данного приложения до степени, допустимой (или приемлемой) для владельца приложения, то задача завершена, и следует обработка риска. Если информации недостаточно, будет проводиться другая итерация оценки риска с пересмотренными критериями риска и средой приложения (например, бизнес-контекст, регулятивный и технологический контексты, спецификации приложения, критерии оценивания риска, критерии принятия риска, критерии воздействия и т. д.), возможно, для ограниченных частей в пределах приложения.

Эффективность обработки риска зависит от результатов оценки риска. Если риск и выведенные требования безопасности для приложения плохо идентифицированы, то адекватная защита приложения не будет обеспечиваться, поскольку требования безопасности необходимы для идентификации целевого уровня доверия приложения (см. 8.2.3). Возможно, что обработка риска не будет сразу же приводить к допустимому (или приемлемому) остаточному риску. В этом случае проводится другая итерация оценки риска с более точными параметрами контекста (например, спецификации приложения, требования безопасности, уровень доверия, необходимые меры и средства контроля и управления безопасностью приложений и т. д.). При необходимости может потребоваться проведение формальной внутренней или внешней валидации.

Согласно ИСО/МЭК 27005, принятие риска происходит в конце процесса менеджмента риска. Поскольку безопасность приложения не может быть осуществлена в конце этапа реализации приложения, то принятие риска приложения должно осуществляться владельцем приложения в более ранний момент ASMP. Это должно происходить в конце процесса оценки риска, когда владелец приложения идентифицирует целевой уровень доверия для конкретного приложения.

В течение всего процесса менеджмента риска безопасности приложений важно, что риски и информация об уровне доверия и взаимосвязанных ASC доводятся до сведения соответствующих групп. Владелец приложения должен также обеспечивать уверенность в проведении мониторинга и рассмотрение риска в течение всего жизненного цикла приложения.

Осведомленность руководства и персонала о рисках, характере имеющихся мер и средств контроля и управления для уменьшения рисков и проблемных областей организации позволяет наиболее эффективным способом бороться с инцидентами и неожиданными событиями. Как определено в ИСО/МЭК 27005, следует документально оформлять подробные результаты каждой деятельности процесса менеджмента риска и результаты принятия решения относительно риска по двум точкам.

Приложение ДА
(справочное)

Сведения о соответствии ссылочных международных стандартов национальным стандартам Российской Федерации

Таблица ДА.1

Обозначение ссылочного международного стандарта	Степень соответствия	Обозначение и наименование соответствующего национального стандарта
ИСО/МЭК 27000:2009	IDT	ГОСТ Р ИСО/МЭК 27000—2012 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология»
ИСО/МЭК 27001:2005	IDT	ГОСТ Р ИСО/МЭК 27001—2006 «Информационная технология. Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Требования»
ИСО/МЭК 27002:2005	IDT	ГОСТ Р ИСО/МЭК 27002—2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности»
ИСО/МЭК 27005:2011	—	*

* Соответствующий национальный стандарт отсутствует. До его утверждения рекомендуется использовать перевод на русский язык данного международного стандарта. Перевод данного международного стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

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

- IDT — идентичные стандарты.

Библиография

[1] ISO/IEC 2382-7:2000, Information technology — Vocabulary — Part 7: Computer programming (ИСО/МЭК 2382-7:2000, Информационные технологии. Словарь. Часть 7. Компьютерное программирование)*

[2] ISO 9000:2005, Quality management systems — Fundamentals and vocabulary (ИСО 9000:2005, Системы менеджмента качества. Основные положения и словарь) *

[3] ISO/IEC TR 9126 (all parts), Software engineering — Product quality

[4] ISO/IEC 12207:2008, Systems and software engineering — Software life cycle processes

[5] ISO/TS 15000 (all parts), Electronic business eXtensible Markup Language (ebXML)

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

[7] ISO/IEC 15288:2008, Systems and software engineering — System life cycle processes

[8] ISO/IEC 15289:2006, Systems and software engineering — Content of systems and software life cycle process information products (Documentation) (ИСО/МЭК 15289:2006, Системная и программная инженерия. Содержание информационных продуктов процесса жизненного цикла систем и программного обеспечения (документация))*

[9] ISO/IEC 15408-3:2008, Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components

[10] ISO/IEC TR 15443 (all parts), Information technology — Security techniques — A framework for IT security assurance

[11] ISO/IEC 18019:2004, Software and system engineering — Guidelines for the design and preparation of user documentation for application software

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

[13] ISO/IEC 21827:2008, Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®) (ИСО/МЭК 21827:2008, Информационная технология. Методы и средства обеспечения безопасности. Проектирование безопасности систем. Модель зрелости процесса (SSE-CMM®))*

[14] ISO/IEC/IEEE 24765:2010, Systems and software engineering — Vocabulary

[15] ISO/IEC/IEEE 29148, Systems and software engineering — Life cycle processes — Requirements engineering

[16] ISO/IEC TR 29193 (в процессе разработки), Secure system engineering principles and techniques

[17] NIST Special Publication 800-48:2008, Guide to Securing Legacy IEEE 802.11 Wireless Networks

[18] NIST Special Publication 800-53 Revision 3:2009, Recommended Security Controls for Federal Information Systems and Organizations

[19] NIST Special Publication 800-77:2005, Guide to SSL VPNs

[20] NIST Special Publication 800-94:2007, Guide to Intrusion Detection and Prevention Systems (IDPS)

[21] NIST Special Publication 800-97:2007, Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i

* Официальный перевод этого стандарта находится в Федеральном информационном фонде технических регламентов и стандартов.

УДК 006.35:004.056.5:004.057.2:006.354 ОКС 35.040

Ключевые слова: информационная технология, безопасность приложений, проект приложения, контекст приложения, жизненный цикл приложения, мера и средство контроля и управления безопасностью приложения, уровень доверия приложения, нормативная структура приложения

Редактор *Н.Н. Кузьмина*
Технический редактор *В.Н. Прусакова*
Корректор *Ю.М. Прокофьева*
Компьютерная верстка *Е.Е. Кругова*

Сдано в набор 10.03.2015. Подписано в печать 25.08.2015. Формат 60 ×84 1/8. Гарнитура Ариал.
Усл. печ. л. 8,37. Уч.-изд. л. 7,95. Тираж 49 экз. Зак. 2867.

Издано и отпечатано во ФГУП «СТАНДАРТИНФОРМ», 123995 Москва, Гранатный пер., 4.

gost.e-ecolog.ru gost.e-ecolog.ru

gost.e-ecolog.ru