ФЕДЕРАЛЬНОЕ АГЕНТСТВО

ПО ТЕХНИЧЕСКОМУ РЕГУЛИРОВАНИЮ И МЕТРОЛОГИИ

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГОСТ Р ИСО/МЭК 27034-6— 2021

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность приложений

Часть 6

Практические примеры

(ISO/IEC 27034-6:2016, IDT)

Издание официальное

Москва
Стандартинформ
2021

Предисловие

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

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

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ Приказом Федерального агентства по техническому регулированию и метрологии от 18 мая 2021 г. № 369-ст

4 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 27034-6:2016 «Информационные технологии. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 6. Практические примеры» (ISO/IEC 27034-6:2016 «Information technology — Security techniques — Application security — Part 6: Case studies», IDT).

ИСО/МЭК 27034-6:2016 подготовлен подкомитетом 27 «Методы и средства обеспечения безопасности ИТ» Совместного технического комитета ИСО/МЭК СТК 1 «Информационные технологии»

5 ВВЕДЕН ВПЕРВЫЕ

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

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

Содержание

Введение

0.1 Общие положения

В настоящее время организации сталкиваются с постоянно растущей потребностью в защите своей информации на уровне приложений. Системный подход к повышению уровня безопасности приложений способствует обеспечению в организации надежной защиты информации, которая используется и хранится в приложениях.

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

Одним из ключевых компонентов настоящего стандарта являются меры обеспечения безопасности приложений (МОБП).

Чтобы облегчить внедрение мер обеспечения безопасности приложений, а также механизмов передачи и обмена данными МОБП, приведенных в ИСО/МЭК 27034 (все части), необходимо определить формальную структуру МОБП и других компонентов этой структуры.

0.2 Назначение

Целью настоящего стандарта является предоставление рекомендаций по применению мер обеспечения безопасности[1)], с помощью которых организации смогут приобретать, разрабатывать, передавать на аутсорсинг и управлять системой безопасности своих приложений в течение всего их жизненного цикла.

0.3 Целевая аудитория

0.3.1 Общие положения

Настоящий стандарт полезен для следующих групп лиц при осуществлении ими своих организационных ролей:

a) эксперты в предметной области.

0.3.2 Эксперты в предметной области

Эксперты в предметной области предоставляют знания, необходимые для подготовки, эксплуатации и аудита приложений. Эксперты должны:

a) участвовать в разработке, валидации и верификации МОБП;

b) участвовать во внедрении и поддержке МОБП, предлагая стратегии, компоненты и процессы внедрения для адаптации МОБП к условиям организации;

c) подтверждать, что МОБП пригодны для применения и несут выгоду в рамках проектов приложений.

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

НАЦИОНАЛЬНЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ

Информационные технологии

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Безопасность приложений

Часть 6

Практические примеры

Information technology. Security techniques.
Application security. Part 6. Case studies

Дата введения — 2021—11—30

1 Область применения

В настоящем стандарте приведены примеры использования МОБП в определенных приложениях.

Примечание — Указанные МОБП приведены только в справочных целях, для обеспечения безопасности приложений рекомендуется разработать собственные МОБП.

2 Нормативные ссылки

В настоящем стандарте отсутствуют нормативные ссылки.

3 Термины и определения

В настоящем стандарте используются термины и определения по ИСО/МЭК 27034-1.

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

- ИСО, Онлайн просматривающий платформу: доступный в https://www.iso.org/obp;
- МЭК, Electropedia: доступный в http://www.electropedia.org/

4 Обозначения

МОБП — меры обеспечения безопасности приложений (ASC).

ЖЦБП — жизненный цикл безопасности приложений (ASLC).

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

НСО — нормативная структура организации (ONF).

5 Руководство по обеспечению безопасности для конкретного приложения

5.1 Общие положения

Руководящие принципы играют важную роль для организаций, которые планируют внедрить любой передовой опыт или стандарт ИСО, поскольку руководства предоставляют указания по использованию методик или правил, а также содержат распространенные примеры их применения.

Организации получат значительную пользу от применения этого руководства, поскольку в нем содержатся практические примеры формирования структуры МОБП для определенных приложений, использующих рекомендуемую структуру данных XML[1)], приведенную в ИСО/МЭК 27034-5-1, и реализации нормативной структуры организации (НСО).

[1)] Расширяемый язык разметки (XML).

Издание официальное

5.2 Пример меры обеспечения безопасности приложений: анализ исходного кода Java для мобильных приложений

5.2.1 Общие положения

Анализ исходного кода кажется тривиальной задачей; но если приложение содержит тысячи строк кода, то эта процедура может быть неэффективной и (или) слишком дорогой.

В данном примере представлена структура МОБП, разработанная вымышленной организацией под названием ORGANIsation Inc. Эта МОБП выполняет защитную функцию анализа исходного кода.

5.2.2 Назначение

Целью этого подраздела является предоставление простого описания примера МОБП под названием «Анализ исходного кода" для организации, разрабатывающей мобильные приложения Java. Для обеспечения краткости и удобочитаемости информации упрощенное подмножество МОБП представлено на русском языке, но требования к МОБП, установленные в ИСО/МЭК 27034-5, позволяют описывать любой объект МОБП, используя набор символов, как приведено в приложении А (таблица А.1).

5.2.3 Контекст

ORGANIsation Inc. — это международная организация, разрабатывающая мобильные приложения на языке Java для внутреннего использования и по запросу своих клиентов. Офисы ORGANIsation Inc. по разработке программного обеспечения расположены в Монреале, Ванкувере и Москве. Поэтому вся документация по разработке, инструкции и справочные материалы в ORGANIsation должны быть доступны на английском, французском и русском языках.

В ходе внедрения ИСО/МЭК 27034 (все части) в ORGANIsation приоритет отдается разработке МОБП с целью уменьшения уязвимостей в мобильном коде на языке Java. Комитет НСО в ORGANIsation поручает Службе безопасности приложений (Application Security Department, ASD) разработать и представить МОБП для анализа исходного кода Java.

5.2.4 Правила классификации информации в ORGANIsation

В ORGANIsation используются утвержденные внутренние правила классификации информации на четыре уровня:

a) с ограниченным доступом;

b) конфиденциальная;

c) строго конфиденциальная;

d) коммерческая.

5.2.5 Уровни доверия приложений, указанные в библиотеке мер обеспечения безопасности приложений ORGANIsation

Считается, что ORGANIsation провела общую оценку рисков безопасности, для чего разделила свои приложения на шесть категорий в зависимости от степени организационного риска. После этого эксперты в предметной области, уполномоченные комитетом НСО, приняли решение использовать эти категории в качестве шаблона для определения уровней доверия приложений в ORGANIsation. Неформальные определения уровней и метки для каждого уровня доверия приложения приведены в таблице 1.

Таблица 1 — Уровни доверия приложений ORGANIsation

Уровень доверия приложения	Название	Описание
0	Основной	Все приложения ORGANIsation должны соответствовать данному уровню доверия приложения
1	Изолированный — только локальная сеть	Этот уровень доверия приложения относится к приложениям, используемым в изолированных корпоративных сетях, не подключенных к внешним сетям
2	Низкий — Интернет, только общедоступная информация	Этот уровень доверия приложения относится к приложениям с доступом в Интернет, передающим общедоступную информацию, не обеспечивая ее конфиденциальности
3	Средний — Интернет, корпоративные пользователи	Этот уровень доверия приложения относится к приложениям с доступом в Интернет для обработки транзакций, используемым корпоративными пользователями и позволяющим получить доступ к корпоративным сервисам, пользовательским файлам и (или) транзакциям на сумму до 5000 долларов США

Окончание таблицы 1

Уровень доверия приложения	Название	Описание
4	Высокий — безопасные транзакции и защита конфиденциальности данных в Интернете	Этот уровень доверия приложения относится к приложениям с доступом в Интернет для обработки транзакций, используемым корпоративными пользователями и позволяющим получить доступ к личной информации пользователей и (или) транзакциям на сумму от 5000 до 25 000 долларов США
5	Приватный	Этот уровень доверия приложения относится к приложениям для обработки транзакций, которым требуется высокий уровень защиты, привилегированный доступ и (или) безопасное хранилище. Они имеют доступ к важной информации и (или) транзакциям на сумму свыше 25 000 долларов США

5.2.6 Результат

Службе безопасности приложений было поручено выбрать и приобрести инструментальное средство автоматического анализа исходного кода на языке Java с настраиваемыми правилами. После анализа предложений, поступивших от поставщиков, служба выбрала инструментальное средство под названием Efficient-Reviewer, версия 2.2.

В результате проекта были разработаны и внедрены пять МОБП версии 1.0.

Таблица 2 — МОБП ORGANIsation для анализа исходного кода

Идентификатор	Название	Уровень доверия приложения	Описание
ORGANIsation-ASD-042	Анализ исходного кода	Основной. Изолированный — только локальная сеть. Низкий — Интернет, только общедоступная информация. Средний — Интернет, корпоративные пользователи. Высокий — безопасные транзакции и защита конфиденциальности данных в Интернете. Приватный	МОБП предназначена для использования разработчиками при анализе исходного кода приложений Java
ORGANIsation-ASD-043	Классификация кода	Основной. Изолированный — только локальная сеть. Низкий — Интернет, только общедоступная информация. Средний — Интернет, корпоративные пользователи. Высокий — безопасные транзакции и защита конфиденциальности данных в Интернете. Приватный	Классификация всех Java классов в пакетах, необходимых приложению. Каждый класс должен наследовать свою классификацию от информации, которую он обрабатывает, с наивысшим уровнем конфиденциальности
ORGANIsation-ASD-044	Базовый автоматический анализ исходного кода	Основной. Изолированный — только локальная сеть. Низкий — Интернет, только общедоступная информация	МОБП предназначена для использования разработчиками при внедрении процедуры анализа исходного кода Java, отнесенного к классам «Стратегический" и «Критически важный"

Окончание таблицы 2

Идентификатор	Название	Уровень доверия приложения	Описание
ORGANIsation-ASD-045	Расширенный автоматический анализ исходного кода	Средний — Интернет, корпоративные пользователи. Высокий — безопасные транзакции и защита конфиденциальности данных в Интернете. Приватный	МОБП предназначена для использования разработчиками при внедрении процедуры анализа исходного кода Java, отнесенного ко всем классам приложений
ORGANIsation-ASD-046	Экспертиза исходного кода	Высокий — безопасные транзакции и защита конфиденциальности данных в Интернете. Приватный	МОБП предназначена для использования разработчиками при внедрении экспертизы исходного кода Java, отнесенного к классам «Стратегический" и «Критически важный"

Примечание — МОБП с идентификатором «ORGANIsation-ASD-042" является корнем иерархии МОБП для анализа исходного кода.

5.2.7 Заинтересованные стороны ORGANIsation, использующие выбранные меры обеспечения безопасности приложений

Для каждой из МОБП определены соответствующие обязанности.

Примечание — В данном пункте приводятся описания элементов выбранных МОБП в произвольной форме и формальные описания тех же элементов с использованием терминологии XML.

Таблица 3 — Имена и обязанности заинтересованных сторон, использующих МОБП для анализа исходного кода Java

Роль/обязанность	Имя	Примечания/директивы ORGANIsation
Автор	Жюль Верн	
Владелец	Дуглас Адамс	Д. Адамс запросил начать нумерацию МОБП в ORGANIsation с 42
Запрос на создание	Герберт Джордж Уэллс	PDF-версия запроса на создание, в которой объясняется, почему организации требуется эта МОБП, будет включена в каждую МОБП. Для ограничения доступа к МОБП требуется PGP-подпись Г. Уэллса. Необходимо указать дату завершения мероприятия
Проектирование	Жюль Верн	
Валидация	Артур Кларк	
Разработка	Фрэнк Герберт	
Верификация	Рэй Брэдбери, Уильям Гибсон	Мероприятия по обеспечению безопасности, измерению и верификации необходимо проверить на обоих языках
Утверждение	Роберт Хайнлайн	Для ограничения доступа к МОБП требуется PGP-подпись Р. Хайнлайна
Окончательное утверждение владельцем	Дуглас Адамс	Для ограничения доступа к МОБП требуется PGP-подпись владельца
Публикация для обучения	Айзек Азимов	
Активный этап	Мэри Шелли	
Срок действия истек	Не указано	

В каждой МОБП должна содержаться дополнительная информация, включающая в себя координаты каждого участника (отдел, адрес электронной почты, номер телефона, физический адрес) и дату завершения каждого мероприятия.

Структура МОБП позволяет добавлять электронную подпись для каждой из версий МОБП с целью обеспечения целостности данных. Директивы ORGANIsation, приведенные в таблице 3, указывают, какие электронные подписи являются обязательными. Это позволяет убедиться, что критические этапы жизненного цикла МОБП выполнены и соответствуют политике ORGANIsation.

Часть МОБП, защищенная электронными подписями, представлена на рисунке 1 в форме облака.

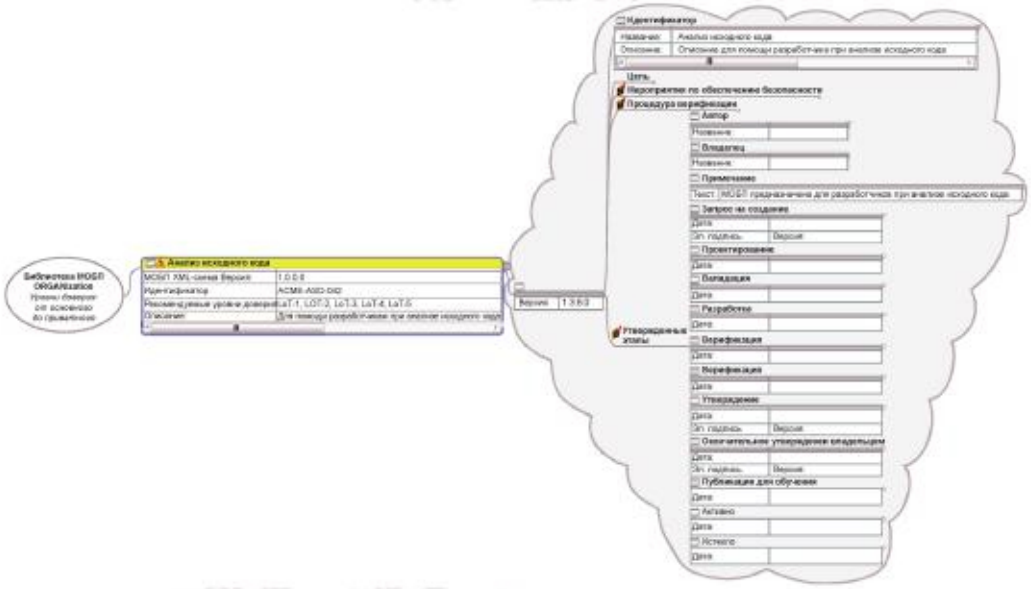

Рисунок 1 — Целостность электронных подписей заинтересованных сторон

Также см. приложение А (таблица А.2).

«МОБП organisation-ASD-042 — анализ исходного кода" является «главной МОБП" и не содержит мероприятий по обеспечению безопасности или проверок и измерений. Она связана с четырьмя дочерними МОБП, которые необходимы для внедрения процедуры анализа исходного кода в процесс разработки приложений Java в организации. Этот принцип иерархии МОБП приведен на рисунке 2. Следует отметить, что в «главной МОБП" пропущены некоторые обязательные атрибуты МОБП, определенные в ИСО/МЭК 27034-1:2011 (рисунок 6). Они содержатся в дочерних МОБП.

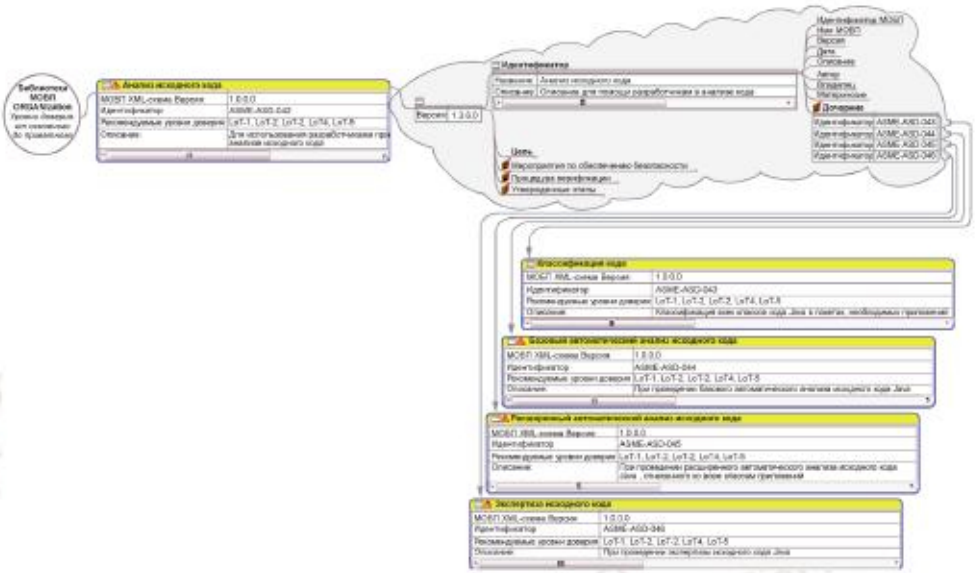

Рисунок 2 — Схема МОБП для анализа исходного кода

Также см. приложение А (таблица А.3).

5.2.8 Описание примеров мер обеспечения безопасности приложений

5.2.8.1 Общие положения

В следующем подпункте описывается «главная МОБП" для анализа исходного кода и ее четыре дочерние МОБП, разработанные и внедренные в библиотеку МОБП ORGANIsation.

5.2.8.2 МОБП ORGANIsation-ASD-042: анализ исходного кода

МОБП	Анализ исходного кода
Уникальный идентификатор МОБП	ORGANIsation-ASD-042
Идентификация	
Уникальный идентификатор МОБП	ORGANIsation-ASD-042
Название МОБП	Анализ исходного кода
Версия	1.3.6.0
Дата	04.01.2016
Описание	МОБП предназначена для использования разработчиками при анализе исходного кода приложений Java
Автор	Жюль Верн Служба безопасности приложений ORGANIsation Inc. 1234 Street ave W, Beautiful city, Quebec, Канада Эл. почта: JVernes@ORGANIsation.com Тел.: +1-234-567-8901

Владелец	Дуглас Адамс Служба безопасности приложений ORGANIsation Inc. 1234 Street ave W, Beautiful city, Quebec, Канада Эл. почта: DAdams@ORGANIsation.com Тел.: +1-109-876-5432
Материнские	—
Дочерние	ORGANIsation-ASD-043; ORGANIsation-ASD-044; ORGANIsation-ASD-045; ORGANIsation-ASD-046

Также см. приложение А (таблица А.4).

Этапы утверждения	(См. пример этапов утверждения МОБП на языке XML в 5.2.7.)		
Цель			
Описание цели	МОБП верхнего уровня, целью которой является группирование различных дочерних МОБП, связанных с анализом исходного кода Java		
Связанные требования	Содержание удалено для упрощения текста документа		
Присвоенные уровни доверия	0, 1, 2, 3, 4, 5		
Контекст использования	Технологический контекст		
Диапазон уровней доверия приложений	Уровень доверия приложения	Название	Описание
	0	Основной	Все приложения ORGANIsation должны соответствовать данному уровню доверия приложения
	1	Изолированный — только локальная сеть	Этот уровень доверия приложения относится к приложениям, используемым в изолированных корпоративных сетях, не подключенных к внешним сетям
	2	Низкий — Интернет, только общедоступная информация	Этот уровень доверия приложения относится к приложениям с доступом в Интернет, передающим общедоступную информацию, не обеспечивая ее конфиденциальности
	3	Средний — Интернет, корпоративные пользователи	Этот уровень доверия приложения относится к приложениям с доступом в Интернет для обработки транзакций, используемым корпоративными пользователями и позволяющим получить доступ к корпоративным сервисам, пользовательским файлам и (или) транзакциям на сумму до 5000 долларов США
	4	Высокий — безопасные транзакции и защита конфиденциальности данных в Интернете	Этот уровень доверия приложения относится к приложениям с доступом в Интернет для обработки транзакций, используемым корпоративными пользователями и позволяющим получить доступ к личной информации пользователей и (или) транзакциям на сумму от 5000 до 25 000 долларов США
	5	Приватный	Этот уровень доверия приложения относится к приложениям для обработки транзакций, которым требуется высокий уровень защиты, привилегированный доступ и (или) безопасное хранилище. Они имеют доступ к важной информации и (или) транзакциям на сумму свыше 25 000 долларов США

	(См. таблицу 2.)
Предварительные условия	Содержание удалено для упрощения текста документа

Также см. приложение А (таблица А.5).

Мероприятие по обеспечению безопасности	Отсутствует
Процедура верификации	Отсутствует

5.2.8.3 МОБП ORGANIsation-ASD-043: классификация кода

МОБП	Классификация кода
Идентификатор МОБП	ORGANIsation-ASD-043
Идентификация	
Уникальный идентификатор МОБП	ORGANIsation-ASD-043
Название МОБП	Классификация кода
Дата	25.12.2015
Описание	Классификация всех Java классов в пакетах, необходимых приложению. Каждый класс должен наследовать свою классификацию от информации, которую он обрабатывает, с наивысшим уровнем конфиденциальности
Версия	2.6.1.1
Автор	Содержание удалено для упрощения текста документа
Владелец	Содержание удалено для упрощения текста документа
Материнские	ORGANIsation-ASD-042
Дочерние	—

Этапы утверждения	(См. пример этапов утверждения МОБП на языке XML в 5.2.7.)

Цель	
Описание цели	Определить объем работ при анализе исходного кода
Связанные требования	Деловые требования: Правила ORGANIsation по разработке, версия 2.1, раздел 5.6 «Классификация компонентов приложения"
Присвоенные уровни доверия приложений	0, 1, 2, 3, 4, 5
Диапазон уровней доверия приложений	(См. таблицу 2.)
Предварительные условия	Содержание удалено для упрощения текста документа

Также см. приложение А (таблица А.6).

Мероприятие по обеспечению безопасности	
Название (что)	Классификация классов и пакетов
Описание	Определение и классификация классов и пакетов приложений Java
Целевая информационная группа	Сведения о приложении [см. ИСО/МЭК 27034-1:2011 (подраздел 6.3)]
Целевая информационная подгруппа	Документация по разработке
Название целевой информационной группы	Архитектура приложений Java

Общее описание результата	Информация о классифицированных классах и пакетах приведена в документации по архитектуре приложений Java
Задействованный эксперт	Орсон Скотт Кард ORGANIsation Inc. Эл. почта: Orson.Scott.Card@ORGANIsation.com
Сложность	ВЫСОКАЯ
Описание сложности	Это мероприятие должно выполняться лицом, которое на основании документов об архитектуре приложения может определить, какой информацией управляет каждый класс Java, а также выявить угрозы, которые могут угрожать конфиденциальной информации
Предполагаемый общий объем работ (сколько)	В среднем 1 ч на классификацию и документирование десяти классов Java. В среднем 15 ч на обновление анализа рисков безопасности приложений
Роль (кто)	АРХИТЕКТОР ПРИЛОЖЕНИЯ
Ответственность	ОТВЕТСТВЕННОЕ ЛИЦО
Требуемая квалификация	1 Сданные экзамены по самым эффективным методикам программирования на Java в ORGANIsation. 2 Не менее пяти лет опыта в разработке приложений Java. 3 Активная сертификация CSSLP[1)]
Предварительное условие	Раздел с определениями классов и пакетов приложений в документации по разработке приложений заполнен. Список классифицированных информационных групп, связанных с приложением, уже создан
Описание мероприятия обеспечения безопасности (как)	Классифицировать классы приложений, которые будут разрабатываться или поддерживаться в этом проекте: 1 определить контексты, роли и информацию, связанную с модулем приложения. Дополнительные материалы: Правила ORGANIsation по разработке приложений, версия 2.1; 2 провести или обновить анализ рисков безопасности приложений; 3 указать все классы в пакетах, необходимых приложению, в разделе «Классификация классов приложений" в документации по разработке приложений. Дополнительные материалы: Руководство ORGANIsation по классификации кода, версия 1.4. Раздел «Классификация классов приложений", шаблон 2.3
Локализация (где)	Среда разработки приложений
Время (когда)	ПОСЛЕ: составление подробной архитектуры приложения
Сопроводительная документация	1 Правила ORGANIsation по разработке приложений, версия 2.1, PDF[2)]. 2 Руководство ORGANIsation по классификации кода, версия 1.4, PDF. 3 Раздел «Классификация классов приложений", шаблон 2.3. RTF[3)]-файл
Программные компоненты (что)	1 Документ: раздел «Классификация модулей приложений" в документации по разработке приложения, описывающий значение классов всех модулей приложений от «Не критичный" до «Критически важный". 2 Документ: метод, шаблоны и примеры классификации описаны в «Руководстве по классификации", ссылка на которое приведена в данной МОБП

Также см. приложение А (таблица А.7).

Процедура верификации	
Название (что)	Верификация классификации классов и пакетов
Описание	Убедиться, что созданные или измененные классы и пакеты приложений Java должным образом классифицированы
Целевая информационная группа	Сведения о приложении [см. ИСО/МЭК 27034-1:2011 (подраздел 6.3)]

[1)] Сертифицированный специалист по безопасному жизненному циклу программного обеспечения (CSSLP).
[2)] Формат электронных документов (формат PDF).
[3)] Формат электронных документов (формат RTF).

Целевая информационная подгруппа	Документация по разработке приложений
Название целевой информационной группы	Архитектура приложений Java
Общее описание результата	Создание или обновление двух документов: анализа рисков безопасности приложений и документации по разработке приложений
Задействованный эксперт	Рэй Брэдбери Эл. почта: Ray.Bradbury @ORGANIsation.com
Сложность	ВЫСОКАЯ
Описание сложности	Это мероприятие должно выполняться лицом, которое на основании документов об архитектуре приложения может определить, какой информацией управляет каждый класс Java, а также выявить угрозы, которые могут угрожать конфиденциальной информации
Предполагаемый общий объем работ (сколько)	В среднем 6 ч на проверку контекста и пересмотр анализа рисков и в среднем 10 мин на утверждение/отклонение каждого класса или пакета. Около 12 ч на проект
Описание мероприятия	Классифицировать классы и компоненты приложений. Дополнительные материалы: Руководство ORGANIsation по классификации кода, версия 1.4
Роль (кто)	АРХИТЕКТОР БЕЗОПАСНОСТИ ПРИЛОЖЕНИЙ
Ответственность	ОТВЕТСТВЕННОЕ И ПОДОТЧЕТНОЕ ЛИЦО
Требуемая квалификация	1 Сданные экзамены по самым эффективным методикам программирования на Java в ORGANIsation. 2 Сданные экзамены по архитектуре безопасности приложений. 3 Активная сертификация CSSLP
Предварительное условие	Документация по архитектуре приложений Java содержит полную информацию о классификации классов и пакетов
Описание мероприятия по верификации и измерению (как)	Пересмотреть и утвердить раздел «Классификация модулей приложений" в документации по разработке приложений: 1 проверить контексты, роли и информацию, связанную с этим модулем; 2 пересмотреть анализ рисков приложений; 3 отклонить или утвердить классификацию каждого класса и внести соответствующую отметку
Локализация (где)	Среда разработки приложений
Время (когда)	До начала написания кода
Сопроводительная документация	1 Руководство ORGANIsation по классификации кода, версия 1.4, PDF
Программные компоненты (что)	1 Обновленный анализ рисков безопасности приложений. 2 Утвержденный раздел «Классификация модулей приложений" в документации по разработке приложений

Также см. приложение А (таблица А.8).

5.2.8.4 МОБП ORGANIsation-ASD-044: базовый автоматический анализ исходного кода

МОБП	Базовый автоматический анализ исходного кода
Идентификатор МОБП	ORGANIsation-ASD-044
Идентификация	
Уникальный идентификатор МОБП	ORGANIsation-ASD-044
Название МОБП	Базовый автоматический анализ исходного кода
Версия	1.3.0.0
Дата	25.12.2015
Описание	МОБП предназначена для использования разработчиками при внедрении автоматической процедуры анализа исходного кода Java, отнесенного к классам «Стратегический" и «Критически важный"

Автор	Содержание удалено для упрощения текста документа
Владелец	Содержание удалено для упрощения текста документа
Материнские	ORGANIsation-ASD-042
Дочерние	—
Этапы утверждения	(См. пример этапов утверждения МОБП на языке XML в 5.2.7.)
Цель	
Описание цели	Предоставление определений (и процедур проверки) для мероприятий, связанных с базовым автоматическим анализом исходного кода
Связанные требования	1 Это средство управления необходимо в соответствии с PCI-DSS 2.0, раздел xx.xx
Присвоенные уровни доверия приложений	0, 1, 2
Контекст использования	Технологический контекст
Диапазон уровней доверия приложений	(См. таблицу 2.)
Предварительные условия	Выполнена классификация всех Java классов в пакетах, необходимых приложению
Мероприятие по обеспечению безопасности	
Название (что)	Автоматический анализ исходного кода (базовый)
Описание	Запустить автоматический анализ исходного кода только для классов «Стратегический" и «Критически важный"
Целевая информационная группа	Данные приложения
Целевая информационная подгруппа	Исходный код
Название целевой информационной группы	Классы и пакеты Java
Общее описание результата	Отчеты об анализе исходного кода, созданные инструментальным средством
Задействованный эксперт	Руководитель группы разработчиков
Сложность	СРЕДНЕЕ
Описание сложности	Перед запуском автоматического анализа исходного кода Java разработчик должен проверить версию файла правил, загруженного в инструментальное средство
Предполагаемый общий объем работ (сколько)	В среднем 20 мин на класс
Роль (кто)	РАЗРАБОТЧИК
Ответственность	ОТВЕТСТВЕННОЕ ЛИЦО
Требуемая квалификация	1 Более 3 мес опыта программирования на Java. 2 Сданные экзамены по работе с инструментальными средствами для анализа исходного кода. 3 Сданные экзамены по самым эффективным методикам программирования на Java в ORGANIsation
Предварительное условие	На пользовательской станции установлено и настроено приложение Efficient-Reviewer версии 2.2
Описание мероприятия обеспечения безопасности (как)	Запустить модульное тестирование всех разработанных классов Java, классифицированных как «Стратегический" и «Критически важный", в инструментальном средстве для анализа исходного кода. 1 Разработчик должен завершить написание кода и выполнить компиляцию класса без ошибок.

	2 Запустить инструментальное средство для анализа исходного кода и загрузить файл правил XXXY-053-JAVA. 3 Выполнить автоматический анализ исходного кода. 4 Сохранить отчет, созданный инструментальным средством для анализа исходного кода. 5 Проанализировать отчет и исправить все обнаруженные ошибки и предупреждения. 6 Создать единый хеш-код из кода Java и созданных файлов отчетов. 7 Вывести хеш-код и отчет с кодом Java
Локализация (где)	Рабочая станция разработчика
Время (когда)	ДО: УРОВЕНЬ ПРИЛОЖЕНИЯ, ЭТАП РЕАЛИЗАЦИИ, МЕРОПРИЯТИЕ ПО РАЗРАБОТКЕ, МЕРОПРИЯТИЕ ПО НАПИСАНИЮ КОДА, КОМПИЛИРОВАНИЕ КОДА
Сопроводительная документация	1 Файл: XXXY-053-JAVA.rules
Программные компоненты (что)	1 Отчет о безопасности без ошибок и предупреждений. 2 Вывод с проверенным кодом, созданным инструментальным средством отчетом и хеш-кодом этих двух файлов
Процедура верификации	
Название (что)	Верификация базового автоматического анализ исходного кода
Описание	Проверить отчеты, созданные инструментальным средством для анализа исходного кода по всем объектам классов «Стратегический" и «Критически важный" в этом модуле проекта приложения
Целевая информационная группа	Данные приложения
Целевая информационная подгруппа	Исходный код
Название целевой информационной группы	Подписанные классы и пакеты Java. Отчет инструментальных средств для анализа исходного кода
Описание целевой информационной группы	После завершения анализа инструментальное средство подпишет исходный код и сохранит подпись в отчете. Файл с исходным кодом, отчет и подпись должны быть верифицированы
Общее описание результата	Модули целевого кода проходят верификацию или отклоняются. После верификации их переносят в среду для «предварительных тестов"
Задействованный эксперт	Руководитель группы разработчиков
Сложность	НИЗКАЯ
Описание сложности	Перед началом верификации необходимо убедиться, что инструментальное средство для создания отчетов находится в той же папке, что и соответствующий исходный код
Предполагаемый общий объем работ (сколько)	В среднем 4 ч на миграцию
Роль (кто)	АУДИТОР
Ответственность	ОТВЕТСТВЕННОЕ ЛИЦО
Требуемая квалификация	Пройденное обучение ORGANIsation по миграции компонентов
Предварительное условие	На сервере с исходным кодом проекта необходимо установить модуль приложения Efficient-Reviewer версии 2.2 «Валидация хеш-кода"
Описание мероприятия обеспечения безопасности (как)	Проверить отчеты, созданные инструментальным средством для анализа исходного кода по всем объектам классов «Стратегический" и «Критически важный" в этом модуле проекта приложения, и перенести их в среду для «предварительных тестов". Используя инструментальное средство для анализа исходного кода Efficient-Reviewer версии 2.2, необходимо: 1 Определить пакеты для миграции. 2 Для каждого из пакетов: а) убедиться, что для каждого класса имеется отчет в журнале;

	b) убедиться, что отчеты не содержат ошибок и предупреждений. Если это так, то необходимо: i) проверить правильность хеш-кода файла пакета и файла отчета, созданных инструментальным средством для анализа исходного кода; ii) если код правильный, отметить файл пакета как «Проверенный" в системе управления версиями. Если это не так, то необходимо: iii) если код неправильный, отметить файл пакета как «Отклоненный" в системе управления версиями; iv) отправить электронное письмо разработчику. 3 Проверить, отмечены ли все файлы пакета как «Проверенные". Если это так, то необходимо: a) осуществить миграцию модуля; b) отправить электронное письмо менеджеру проектов. Если это не так, то необходимо: a) отменить миграцию; b) отправить электронное письмо менеджеру проектов
Локализация (где)	Среда разработки, сервер с исходным кодом проекта
Время (когда)	ДО УРОВНЯ ДОСТАВКИ ПРИЛОЖЕНИЯ, ЭТАПА ПЕРЕХОДА, МИГРАЦИИ МОДУЛЯ В СРЕДУ ДЛЯ ТЕСТОВ
Программные компоненты (что)	Список пакетов проекта приложения в этом модуле с обновленным статусом

5.2.8.5 МОБП ORGANIsation-ASD-045: расширенный автоматический анализ исходного кода

МОБП	Расширенный автоматический анализ исходного кода
Идентификатор МОБП	ORGANIsation-ASD-045
Идентификация	
Уникальный идентификатор МОБП	ORGANIsation-ASD-045
Название МОБП	Расширенный автоматический анализ исходного кода
Дата	25.12.2015
Описание	МОБП предназначена для использования разработчиками при внедрении автоматической процедуры анализа исходного кода Java, отнесенного ко всем классам приложений
Версия	1.0.0.0
Автор	Содержание удалено для упрощения текста документа
Владелец	Содержание удалено для упрощения текста документа
Материнские	ORGANIsation-ASD-042
Дочерние	—
Этапы утверждения	(См. пример этапов утверждения МОБП на языке XML в п. 5.2.7.)
Цель	
Описание цели	Предоставление определений (и процедур проверки) для мероприятий, связанных с расширенным автоматическим анализом исходного кода
Связанные требования	Это средство управления необходимо в соответствии с PCI-DSS 2.0, раздел xx.xx
Присвоенные уровни доверия приложений	3, 4, 5
Диапазон уровней доверия приложений	(См. таблицу 2.)
Предварительные условия	Выполнена классификация всех Java классов в пакетах, необходимых приложению
Мероприятие по обеспечению безопасности	
Название (что)	Автоматический анализ исходного кода (расширенный)

Описание	Запустить полный автоматический анализ исходного кода всех классов Java, написанных разработчиком
Целевая информационная группа	Данные приложения
Целевая информационная подгруппа	Исходный код
Название целевой информационной группы	Классы и пакеты Java
Общее описание результата	Отчеты об анализе исходного кода, созданные инструментальным средством
Задействованный эксперт	Руководитель группы разработчиков
Сложность	СРЕДНЕЕ
Описание сложности	Перед запуском автоматического анализа исходного кода Java разработчик должен проверить версию файла правил, загруженного в инструментальное средство
Предполагаемый общий объем работ (сколько)	В среднем 20 мин на класс
Роль (кто)	РАЗРАБОТЧИК
Ответственность	ОТВЕТСТВЕННОЕ ЛИЦО
Требуемая квалификация	1 Более 3 мес опыта программирования на Java. 2 Сданные экзамены по работе с инструментальными средствами для анализа исходного кода. 3 Сданные экзамены по самым эффективным методикам программирования на Java в ORGANIsation
Предварительное условие	На пользовательской станции установлено и настроено приложение Efficient-Reviewer версии 2.2
Описание мероприятия обеспечения безопасности (как)	Запустить модульное тестирование всех разработанных классов Java в инструментальном средстве для анализа исходного кода. 1 Разработчик должен завершить написание кода и выполнить компиляцию класса без ошибок. 2 Запустить инструментальное средство для анализа исходного кода и загрузить файл правил XXXY-053-JAVA. 3 Выполнить автоматический анализ исходного кода. 4 Сохранить отчет, созданный инструментальным средством для анализа исходного кода. 5 Проанализировать отчет и исправить все обнаруженные ошибки и предупреждения. 6 Создать единый хеш-код из кода Java и созданных файлов отчетов. 7 Вывести хеш-код и отчет с кодом Java
Локализация (где)	Рабочая станция разработчика
Время (когда)	ДО: УРОВЕНЬ ПРИЛОЖЕНИЯ, ЭТАП РЕАЛИЗАЦИИ, МЕРОПРИЯТИЕ ПО РАЗРАБОТКЕ, МЕРОПРИЯТИЕ ПО НАПИСАНИЮ КОДА, КОМПИЛИРОВАНИЕ КОДА
Сопроводительная документация	1 Файл: XXXY-053-JAVA.rules
Программные компоненты (результат)	1 Созданный отчет о безопасности без ошибок и предупреждений. 2 Вывод с проверенным кодом, созданным инструментальным средством отчетом и хеш-кодом этих двух файлов
Процедура верификации	
Название (что)	Верификация расширенного автоматического анализа исходного кода
Описание	Проверить отчеты, созданные инструментальным средством для анализа исходного кода по всем объектам классов «Стратегический" и «Критически важный" в этом модуле проекта приложения
Целевая информационная группа	Данные приложения

Название целевой информационной группы	Данные приложения
Целевая информационная подгруппа	Исходный код
Описание целевой информационной группы	Подписанные классы и пакеты Java. Отчет инструментальных средств для анализа исходного кода
Классификация целевой информационной группы	После завершения проверки инструментальное средство подпишет исходный код и сохранит подпись в отчете. Файл с исходным кодом, отчет и подпись должны быть верифицированы
Общее описание результата	Модули целевого кода проходят верификацию или отклоняются. После верификации их переносят в среду для «предварительных тестов"
Задействованный эксперт	Руководитель группы разработчиков
Сложность	НИЗКАЯ
Описание сложности	Перед началом верификации необходимо убедиться, что инструментальное средство для создания отчетов находится в той же папке, что и соответствующий исходный код
Предполагаемый общий объем работ (сколько)	В среднем 10 ч на миграцию
Роль (кто)	АУДИТОР
Ответственность	ОТВЕТСТВЕННОЕ ЛИЦО
Требуемая квалификация	Пройденное обучение ORGANIsation по миграции компонентов
Предварительное условие	На пользовательской станции установлен и настроен модуль приложения Efficient-Reviewer версии 2.2 «Валидация хеш-кода"
Описание мероприятия обеспечения безопасности (как)	Проверить отчеты, созданные инструментальным средством для анализа исходного кода по объектам всех классов в этом модуле проекта приложения и перенести их в среду для «предварительных тестов". Используя инструментальное средство для анализа исходного кода Efficient-Reviewer версии 2.2, необходимо: 1 Определить пакеты для миграции. 2 Для каждого из пакетов: a) убедиться, что для каждого класса имеется отчет в журнале; b) убедиться, что в отчетах отсутствуют ошибки и предупреждения. Если это так, то необходимо: i) проверить правильность хеш-кода файла пакета и файла отчета, созданных инструментальным средством для анализа исходного кода; ii) если код правильный, отметить файл пакета как «Проверенный" в системе управления версиями. Если это не так, то необходимо: i) если код неправильный, отметить файл пакета как «Отклоненный" в системе управления версиями; ii) отправить электронное письмо разработчику. 3 Проверить, отмечены ли все файлы пакета как «Проверенные"? Если это так, то необходимо: a) осуществить миграцию модуля; b) отправить электронное письмо менеджеру проектов. Если это не так, то необходимо: a) отменить миграцию; b) отправить электронное письмо менеджеру проектов
Локализация (где)	Среда разработки, сервер с исходным кодом проекта
Время (когда)	ДО УРОВНЯ ДОСТАВКИ ПРИЛОЖЕНИЯ, ЭТАПА ПЕРЕХОДА, МИГРАЦИИ МОДУЛЯ В СРЕДУ ДЛЯ ТЕСТОВ
Программные компоненты (результат)	Список пакетов проекта приложения в этом модуле с обновленным статусом

5.2.8.6 МОБП ORGANIsation-ASD-046: экспертиза исходного кода

МОБП	Экспертиза исходного кода
Идентификатор МОБП	ORGANIsation-ASD-046
Идентификация	
Уникальный идентификатор МОБП	ORGANIsation-ASD-046
Название МОБП	Экспертиза исходного кода
Версия	3.5.0.2
Дата	07.09.2014
Описание	МОБП предназначена для использования разработчиками при внедрении экспертизы исходного кода Java, отнесенного к классам «Стратегический" и «Критически важный"
Автор	Содержание удалено для упрощения текста документа
Владелец	Содержание удалено для упрощения текста документа
Материнские	ORGANIsation-ASD-042
Дочерние	—
Этапы утверждения	(См. пример этапов утверждения МОБП на языке XML в п. 5.2.7.)
Цель	
Описание цели	Предоставление определений (и процедур проверки) для мероприятий, связанных с экспертизой исходного кода
Связанные требования	Это средство управления необходимо в соответствии с Политикой обеспечения безопасности критически важных приложений ORGANIsation, подраздел 12.6
Рекомендуемый уровень доверия приложения	4, 5
Контекст использования	Технологический контекст
Диапазон уровней доверия приложений	(См. таблицу 2.)
Предварительные условия	Выполнена классификация всех Java классов в пакетах, необходимых приложению
Мероприятие по обеспечению безопасности	
Название (что)	Экспертиза исходного кода
Описание	Выполнить экспертизу исходного кода только для классов «Стратегический" и «Критически важный"
Целевая информационная группа	Данные приложения
Целевая информационная подгруппа	Исходный код
Название целевой информационной группы	Классы и пакеты Java
Общее описание результата	Отчеты об экспертизе исходного кода, созданные рецензентом
Задействованный эксперт	
Сложность	ВЫСОКАЯ
Описание сложности	
Предполагаемый общий объем работ (сколько)	В среднем 14 ч на модуль
Роль (кто)	РУКОВОДИТЕЛЬ ГРУППЫ РАЗРАБОТЧИКОВ
Ответственность	ОТВЕТСТВЕННОЕ ЛИЦО

Требуемая квалификация	1 Сданные экзамены по самым эффективным методикам программирования на Java в ORGANIsation. 2 Не менее пяти лет опыта в разработке приложений Java. 3 Активная сертификация CSSLP
Предварительное условие	На пользовательской станции установлена и настроена последняя версия приложения PGP Desktop Home
Описание мероприятия обеспечения безопасности (как)	1 Получить шаблон отчета об экспертизе исходного кода (прилагается к МОБП). 2 Пройти обучение эффективным методикам безопасного программирования на Java (прилагается к МОБП). 3 Определить элементы классификации. 4 Для каждого класса «Стратегический" и «Критически важный": a) убедиться, что код соответствует внутренним эффективным методикам безопасного программирования на Java; b) заполнить отчет об экспертизе исходного кода, используя шаблон; c) отметить класс как «Подтвержденный" или «Отклоненный"; d) подписать класс и связанный отчет; e) вывести класс и соответствующий отчет. 5 Если любой из классов помечен как «Отклоненный", то: a) открыть запросы на исправление отклоненных классов. b) отправить список отклоненных классов разработчику
Локализация (где)	Рабочая станция разработчика
Время (когда)	ПОСЛЕ: возврата модуля Java разработчиком
Сопроводительная документация	1 Шаблон отчета об экспертизе исходного кода, версия 5.6, docx. 2 Руководство ORGANIsation по безопасному программированию на Java, версия от 2012 г. PDF
Программные компоненты (что)	1 Подписанные рецензентом выведенные классы с обновленным статусом и отчетом об экспертизе исходного кода. 2 Запросы на исправление. 3 Список отклоненных классов
Процедура верификации	
Название (что)	Верификация экспертизы исходного кода
Описание	Проверить отчеты об экспертизе исходного кода по всем объектам классов «Стратегический" и «Критически важный" в этом модуле проекта приложения
Целевая информационная группа	Данные приложения
Целевая информационная подгруппа	Исходный код
Название целевой информационной группы	Данные приложения
Описание целевой информационной группы	Подписанные классы и пакеты Java. Отчет об экспертизе исходного кода
Общее описание результата	Модули целевого кода проходят верификацию или отклоняются
Задействованный эксперт	
Сложность	СРЕДНЕЕ
Описание сложности	
Предполагаемый общий объем работ (сколько)	15 мин на компонент приложения
Роль (кто)	АУДИТОР
Ответственность	ОТВЕТСТВЕННОЕ ЛИЦО
Требуемая квалификация	1 Сданные экзамены по самым эффективным методикам программирования на Java в ORGANIsation. 2 Не менее пяти лет опыта в разработке приложений Java. 3 Активная сертификация CISA

Предварительное условие	На пользовательской станции установлена и настроена последняя версия приложения PGP Desktop Home
Описание мероприятия обеспечения безопасности (как)	Убедитесь, что все классы с отметкой «Стратегический" и «Критически важный" проверены вручную по мере необходимости. 1 Определить пакеты для миграции. 2 Для каждого из пакетов: a) для каждого пакета классов «Стратегический" и «Критически важный" необходимо убедиться, что выведенный класс отмечен как «Проверенный", а класс и связанный отчет подписаны уполномоченным рецензентом кода; b) проверить, удовлетворяют ли все классы в этом пакете вышеуказанным критериям? Если это так, то необходимо: i) отметить пакет как «Проверенный"; ii) отправить электронное письмо менеджеру проектов. Если это не так, то необходимо: i) отметить пакет как «Отмененный"; ii) отправить электронное письмо менеджеру проектов
Локализация (где)	Среда разработки, сервер с исходным кодом проекта
Время (когда)	ДО УРОВНЯ ДОСТАВКИ ПРИЛОЖЕНИЯ, ЭТАПА ПЕРЕХОДА, МИГРАЦИИ МОДУЛЯ В СРЕДУ ДЛЯ ТЕСТОВ
Программные компоненты (что)	1 Список классифицированных компонентов приложения, которые необходимо проверить. 2 Результаты экспертизы исходного кода по каждому из них, включая: a) имя рецензента; b) дату и время проверки; c) утверждение; d) открытый ключ верификатора для проверки подписи исходного кода с целью обеспечения целостности

5.3 Пример использования: разработка мер обеспечения безопасности приложений для решения вопросов конфиденциальности в двух странах

5.3.1 Общие положения

В рамках регулятивного контекста перечисляются и описываются все законы или нормативные акты в любой сфере деятельности организации, которые могут повлиять на проекты приложений. В этот контекст входят законы, правила и нормы юрисдикций и стран, в которых приложения разрабатываются, и (или) развертываются, и (или) используются.

Нормативные вопросы необходимо рассматривать с осторожностью, особенно если в сфере использования приложения действуют противоречащие друг другу законы разных стран или культур. После определения регулятивного контекста приложения можно обнаружить и устранить потенциальные противоречивые правила.

5.3.2 Назначение

Назначение этого подраздела — предоставить пример разработки МОБП для решения вопросов конфиденциальности для двух стран.

5.3.3 Контекст

ORGANIsation Inc. — международная организация, предоставляющая медицинским клиникам услугу ведения медицинских карт в режиме онлайн. Приложение поддерживает функцию автоматического удаления медицинских карт после пяти лет их бездействия.

ORGANIsation нашла новых клиентов в странах A и B.

На первом этапе процесса менеджмента безопасности приложений (ПМБП) юристы ORGANIsation выделили и проанализировали соответствующие законы и правила обеих стран и сформировали регулятивный контекст для приложения. Был обнаружен конфликт между некоторыми требованиями законов о конфиденциальности в странах A и B.

В частности, одна статья закона о конфиденциальности страны A гласит, что персональные данные субъекта следует хранить не менее десяти лет после последнего использования, а в соответствии со статьей закона о конфиденциальности страны B персональные данные субъекта необходимо надежно удалять в течение одного года после последнего использования.

С учетом риска нарушения существующих законов для клиентов ORGANIsation возникает два требования:

a) обеспечить, чтобы в стране A персональные данные субъекта хранились не менее десяти лет после последнего использования;

b) обеспечить, чтобы в стране B персональные данные субъекта надежно удалялись в течение одного года после последнего использования.

ORGANIsation должна продемонстрировать клиентам, что приложение отвечает этим требованиям.

ORGANIsation принимает решение удовлетворить эти требования путем внедрения следующих МОБП.

a) МОБП 1: внедрить процедуру безопасного удаления медицинских карт и связанной с ними информации. Это «головная МОБП", которая служит материнской для двух указанных ниже дочерних МОБП.

1) МОБП 1.1: разработать, внедрить и верифицировать процедуры безопасного удаления.
   i) Когда: ВО ВРЕМЯ подробного анализа архитектуры (уровень доставки приложения, внедрение/разработка/уточнение).
   ii) Мероприятие по обеспечению безопасности: в МОБП должны входить, помимо прочего, следующие мероприятия по обеспечению безопасности:
      - разработка и внедрение безопасной процедуры удаления медицинской карты определенного пациента из базы данных приложения;
      - разработка и внедрение безопасной процедуры удаления файлов, относящихся к медицинской карте определенного клиента, с файловых серверов приложения;
      - разработка и внедрение безопасной процедуры удаления медицинской карты определенного пациента из архивной базы данных и архивных файлов.
   iii) Процедура верификации: в МОБП должны быть описаны процедуры проверки правильности реализации каждого из указанных выше мероприятий.
2) МОБП 1.2: выполнить процедуры безопасного удаления, реализованные в МОБП 1.1, и проверить правильность их работы.
   i) Когда: ВО ВРЕМЯ использования приложения (уровень поставки приложения, эксплуатация и сопровождение/вывод из эксплуатации).
   ii) Мероприятие по обеспечению безопасности: в МОБП должны входить, помимо прочего, следующие мероприятия по обеспечению безопасности:
      - выполнение безопасной процедуры удаления данных при необходимости.
   iii) Процедура верификации: в МОБП должны быть описаны процедуры проверки правильности удаления данных приложением.

b) МОБП 2: внедрить процедуру правильного выбора медицинских карт для удаления согласно соответствующим правилам. Это «главная" МОБП, которая служит материнской для двух указанных ниже дочерних МОБП.

1) МОБП 2.1: разработать, внедрить и верифицировать процедуру правильного выбора медицинских карт для удаления согласно соответствующим правилам.
   i) Когда: ВО ВРЕМЯ подробного анализа архитектуры (уровень поставки приложения, реализация/проектирование/уточнение).
   ii) Мероприятие по обеспечению безопасности: в МОБП должны входить, помимо прочего, следующие мероприятия по обеспечению безопасности:
      - добавление в профиль клиники сведений о стране, в которой она находится;
      - добавление в каждую медицинскую карту поля, в котором указана связанная с ней клиника;
      - добавление в каждую медицинскую карту поля, в котором указано время последнего использования;
      - определение и внедрение правил удаления для каждой из стран;
      - изменение процедуры выбора в приложении с учетом соответствующих правил удаления для каждой медицинской карты.
   iii) Процедура верификации: в МОБП должны быть описаны процедуры проверки правильности реализации каждого из указанных выше мероприятий.
      - В частности, юристы должны подтвердить правила удаления для каждой из стран.
2) МОБП 2.2: выполнить процедуры безопасного удаления, реализованные в МОБП 2.1, и проверить правильность их работы.
   i) Когда: ВО ВРЕМЯ использования приложения (уровень поставки приложения, эксплуатация и сопровождение/вывод из эксплуатации).

ii) Мероприятие по обеспечению безопасности: в МОБП должны входить, помимо прочего, следующие мероприятия по обеспечению безопасности:
- выполнение процедуры выбора данных при необходимости.

iii) Процедура верификации: в МОБП должны быть описаны процедуры проверки правильности выбора данных приложением.

5.4 Пример использования: интеграция сторонних мер обеспечения безопасности приложений

5.4.1 Общие положения

Разработка необходимых МОБП для обеспечения безопасности приложения собственными силами организации может представлять собой сложный и длительный процесс, требующий специальных знаний и ресурсов. Этот процесс можно значительно облегчить, если вместо собственной разработки МОБП приобретать, адаптировать и интегрировать в НСО организации сторонние МОБП.

Необходимым условием для интеграции и адаптации сторонних МОБП является открытый и переносимый язык обмена данными для МОБП (в соответствии с рекомендациями ИСО/МЭК 27034-5-1).

5.4.2 Назначение

Назначение данного примера использования — показать, как сторонние МОБП можно адаптировать и интегрировать в программу обеспечения безопасности приложений организации. Кроме того, данный пример подчеркивает важность включения диапазона уровней доверия приложений в определение МОБП.

Для упрощения описания некоторые пункты в примере определены как «[опущено]", однако в соответствии с рекомендованной XML-структурой из ИСО/МЭК 27034-5-1 их необходимо вносить в каждую МОБП.

5.4.3 Контекст

ORGANIsation Inc. («организация") — это компания, занимающаяся онлайн-торговлей биржевых ценных бумаг, например фьючерсов, облигаций и акций. В настоящее время ORGANIsation использует 80 приложений, 25 из которых подключаются к Интернету. 12 мес назад ORGANIsation запустила программу обеспечения безопасности приложений. В настоящее время НСО состоит из 13 МОБП с четырьмя уровнями доверия приложений (см. таблицу 4).

Таблица 4 — Уровни доверия приложений ORGANIsation

Уровень доверия приложений	Описание
(i)	Приложения с доступом в Интернет, обрабатывающие конфиденциальную информацию
(ii)	Приложения с доступом в Интернет, обрабатывающие только неконфиденциальную информацию
(iii)	Внутренние приложения, обрабатывающие конфиденциальную информацию
(iv)	Внутренние приложения, обрабатывающие только неконфиденциальную информацию

В соответствии с недавними изменениями в регулятивном контексте ORGANIsation необходимо обновить свою НСО, чтобы обеспечить применение различных видов тестирования безопасности своих приложений. Чтобы ускорить процесс обновления НСО, организация решает приобрести две МОБП у стороннего поставщика, а также нанять специалиста по проведению тестирования на проникновение из Hackus Inc. («Hackus").

На рисунке 3, иллюстрирующем пример использования «интеграции сторонней МОБП", показана процедура передачи двух МОБП (МОБП1 и МОБП2) от двух разных субпоставщиков приобретающей стороне («ORGANIsation").

Рисунок 3 — Пример цепочки поставки МОБП

У каждой вовлеченной в процесс организации имеется своя собственная НСО, как показано на рисунке 3. В рамках «Проекта приложения" поставщик предоставляет адаптированную версию своего «Универсального приложения". МОБП «Общего приложения" действуют в своих (отдельных) нормативных структурах приложений (НСП). Эти МОБП входят в НСО поставщика. НСО поставщика получает МОБП1 от специализированной охранной компании («Поставщик МОБП"), а МОБП2 — от одного из субпоставщиков (программных) компонентов («Субпоставщик компонентов"). Хотя МОБП1 и МОБП2 предназначены для использования с «Универсальным приложением" в составе НСП, сначала необходимо интегрировать их в НСО поставщика. Состав и характер средств управления НСП* клиента могут отличаться от общей НСП. НСП* передается приобретающей стороне вместе с «Проектом приложения" в целом. Приобретающая сторона может обновить ее конфигурацию безопасности, создав НСП**. Новые МОБП1 и МОБП2, попавшие в НСП**, также регистрируются в НСО приобретающей стороны. Стрелка на рисунке между НСО приобретающей стороны и НСП проекта приложения направлена в обе стороны, поскольку в новом проекте могут использоваться дополнительные МОБП (например, созданные для определенного сайта).

Путь передачи МОБП1, представленный на рисунке 3, можно описать в виде последовательности: НСО Поставщика МОБП → НСО Поставщика → НСП Поставщика → НСП* Поставщика → НСП** приобретающей стороны → НСО приобретающей стороны. Приобретающая сторона может получить МОБП3 напрямую от поставщика МОБП, который явно не указан на рисунке 3. В соответствии с соглашением о покупке и согласно схеме, приведенной в ИСО/МЭК 27034-5-1, Hackus экспортирует обе МОБП в виде «пакета МОБП" в формате XML. Фрагменты обеих МОБП приведены ниже. Поскольку 5.4 содержит только процедуру интеграции сторонних МОБП в НСО организации, мероприятия по обеспечению безопасности, а также по верификации МОБП опущены.

МОБП 1.1: автоматический поиск уязвимостей.

Когда:

- ВО ВРЕМЯ [12-месячный период] (уровень поставки приложений/ эксплуатации/использования и сопровождения).

Рекомендуемые уровни доверия приложений:

- «Синий" уровень.

Шкала уровней доверия приложения[1]:

- «Синий" уровень: приложения, которые не обрабатывают и не хранят конфиденциальную информацию, а также не получают к ней доступа.

- «Красный" уровень: приложения, которые обрабатывают и хранят конфиденциальную информацию, а также имеют к ней доступ.

Мероприятие по обеспечению безопасности: [опущено]

Мероприятие по верификации: [опущено]

МОБП 1.2: Тестирование на проникновение

Когда:

- ВО ВРЕМЯ [12-месячный период] (уровень поставки приложений/ эксплуатации/использования и сопровождение).

Рекомендуемые уровни доверия:

- «Красный" уровень.

Шкала уровней доверия приложений:

- «Синий" уровень: приложения, которые не обрабатывают и не хранят конфиденциальную информацию, а также не получают к ней доступа.

- «Красный" уровень: приложения, которые обрабатывают и хранят конфиденциальную информацию, а также имеют к ней доступ.

Мероприятие по обеспечению безопасности: [опущено]

Мероприятие по верификации: [опущено]

Согласно шкале уровней доверия приложений, включенной в обе МОБП, Hackus использует два уровня доверия приложения («красный" и «синий"), а ORGANIsation — четыре уровня доверия (i, ii, iii, iv). Для интеграции МОБП в НСО ORGANIsation важно сопоставить уровни доверия приложений Hackus и ORGANIsation. В таблице 5 представлено такое сопоставление.

Таблица 5 — Сопоставление уровней доверия приложений Hackus и ORGANIsation

Hackus	ORGANIsation
Синий	(ii), (iv)
Красный	(i), (iii)

Сопоставление выполнено после рассмотрения определений уровней доверия приложений ORGANIsation и Hackus (в МОБП). При этом становится очевидным, что в структуре НСО ORGANIsation необходимо присвоить МОБП для автоматического поиска уязвимостей уровни доверия приложений (ii) и (iv), а МОБП для проведения тестирования на проникновение — уровни (i) и (III).

5.5 Пример использования: использование эталонной модели жизненного цикла безопасности приложений для упрощения процедуры внедрения мер обеспечения безопасности приложений различными группами разработки внутри организации

5.5.1 Общие положения

В эталонной модели жизненного цикла безопасности приложения (ЭМЖЦБП) приведен «независимый от методологии разработки" справочный список мероприятий и ролей, охватывающих различные этапы и аспекты жизненного цикла приложения. ЭМЖЦБП представляет собой общую основу для всех МОБП и помогает организациям внедрять одинаковые МОБП в разных проектах, командах разработчиков и методологиях разработки.

5.5.2 Назначение

Назначение данного примера использования — показать важность и полезность ЭМЖЦБП. Данный пример демонстрирует, что МОБП можно использовать в различных контекстах разработки с учетом мероприятий по разработке ЭМЖЦБП.

5.5.3 Контекст

ORGANIsation Inc. («ORGANIsation") — это банковская и страховая корпорация национального масштаба. В ней работают более 40 000 сотрудников и несколько внутренних команд разработчиков,

[1] На шкале уровней доверия приложений Hackus в данном примере синий цвет обозначает меньший риск, а красный — больший.

которые используют различные методологии разработки, например Agile и Heavyweight. Цель недавно внедренной инициативы по защите приложений: систематическая интеграция функций безопасности во все проекты с разными методологиями разработки.

С этой целью ORGANIsation разработала 18 МОБП, охватывающих различные аспекты безопасности приложений, например обучение, анализ исходного кода, тестирование и сертификацию. Пример МОБП (тестирование на проникновение) приведен в таблице 6. Для краткости изложения МОБП показана в сокращенной и упрощенной форме.

Таблица 6 — МОБП ORGANIsation для проведения тестирования на проникновение

Название	Тестирование на проникновение
Описание	Тестирование на проникновение — это контролируемая проверка безопасности, целью которой является использование уязвимостей системы для получения (несанкционированного) доступа. Проверка проводится в контролируемой среде экспертом по безопасности (белым хакером) в соответствии с определенными правилами взаимодействия. По результатам каждой проверки составляется подробный отчет, в котором перечисляются найденные уязвимости (эксплоиты) и их критичность
Уровни доверия приложений	МОБП применяется для приложений со следующими уровнями доверия: - критически важный; - высокий
Мероприятие по обеспечению безопасности	
Сложность	Высокая. Как правило, тестирование на проникновение состоит из нескольких модулей, каждый из которых направлен на проверку определенного аспекта или компонента системы. Для каждого модуля может потребоваться несколько сеансов испытаний
Спецификация	Задача 1. Запрос и планирование. Проектный менеджер связывается со службой безопасности, чтобы запросить и запланировать тестирование на проникновение разрабатываемой системы. Время выполнения: (1.1.1.2.14 — PLAN_QUALITY). Распределение ресурсов: проектный менеджер. Задача 2. Объем испытания и правила взаимодействия. Архитектор безопасности вместе с владельцем приложения и проектным менеджером определяют объем испытания (в соответствии с требованиями безопасности), а также правила взаимодействия. Время выполнения: 2.1.3.3.3 (DEFINE_THE_SECURITY_SPECIFICATION). Распределение ресурсов: - архитектор безопасности; - владелец приложения; - проектный менеджер. Конечный результат: - план испытания; - правила взаимодействия. Задача 3. Испытание. Тестировщик проводит тестирование на проникновение в соответствии с планом и правилами взаимодействия. После завершения испытания тестировщик просматривает результаты вместе с архитектором приложения и владельцем приложения и составляет подробный план действий по устранению обнаруженных уязвимостей. Время выполнения: 2.1.3.3.4 (TEST_SOLUTION) Распределение ресурсов: - тестировщик; - архитектор приложения; - владелец приложения. Конечный результат: отчет об уязвимостях, план действий
Процедура верификации	[опущено]

Как приведено в таблице 6, при проведении мероприятий по обеспечению безопасности приложений должны быть решены три задачи. Каждой задаче присваиваются описание, время выполнения,

распределение ресурсов и конечный результат (при необходимости). Хотя описание и конечный результат приведены в произвольной форме, время выполнения и распределение ресурсов указаны в соответствии с ЭМЖЦБП.

Данная форма косвенной адресации позволяет (повторно) использовать МОБП в различных методологиях разработки с разными мероприятиями и ролями. Для этого необходимо сопоставить конкретные роли и мероприятия (определенной методологии разработки) с их аналогами в ЭМЖЦБП. Примеры сопоставления для методологий разработки ORGANIsation Agile и ORGANIsation Heavyweight приведены в таблицах 7 и 8.

Сопоставление жизненного цикла мероприятий.

Таблица 7 — Сопоставление мероприятий ЭМЖЦБП с существующими мероприятиями ORGANIsation

ЭМЖЦБП	ORGANIsation agile	ORGANIsation heavyweight
PLAN_QUALITY	Разработка плана	Составить план проекта
DEFINE_THE_SECURITY_SPECIFICATION	Создание списка требований	Определить дополнительные требования
TEST_SOLUTION	Сбор тестовых данных	Выполнить проверку безопасности

Сопоставление ролей.

Таблица 8 — Сопоставление ролей ЭМЖЦБП с существующими ролями ORGANIsation

ЭМЖЦБП	ORGANIsation agile	ORGANIsation heavyweight
Проектный менеджер	Скрам-мастер	Проектный менеджер
Архитектор безопасности	Специалист по безопасности	Архитектор безопасности
Владелец приложения	Владелец решения	Владелец приложения
Тестировщик	Специалист по тестированию на проникновение	Тестировщик безопасности систем

Благодаря этим сопоставлениям команде разработчиков и экспертам в предметной области МОБП не требуются сведения о мероприятиях и ролях в ORGANIsation Agile, ORGANIsation Heavyweight или любой другой методологии. Им нужны только данные об ЭМЖЦБП.

Отделам разработки приложений, использующим методологию ORGANIsation Agile, не требуется изучать новую методологию, им достаточно изучить соответствие их методологии с ЭМЖЦБП. Им не требуются сведения о мероприятиях и ролях в ORGANIsation Heavyweight или любой другой методологии. То же самое касается других отделов разработки.

5.6 Пример использования: внедрение сторонних мер обеспечения безопасности приложений в процесс безопасного жизненного цикла разработки

5.6.1 Общие положения

Одна из характеристик эффективно управляемой компании — это ее реакция на нештатную ситуацию. Одним из примеров такой реакции является эффективная и продуктивная разработка необходимых МОБП в ответ на замеченную атаку или с целью выявления уязвимостей. Разработка соответствующих МОБП может быть сложной задачей, особенно если в компании отсутствует безопасная среда разработки и связанная библиотека МОБП. Как указано в 5.4, разработка соответствующего набора собственных МОБП может представлять собой сложный и длительный процесс, требующий специальных знаний и ресурсов, и чаще всего не является оптимальным решением в случае атаки. Для обеспечения быстрого и эффективного реагирования на непосредственную угрозу и возможность утечки данных организация может принять решение использовать сторонние МОБП.

5.6.2 Назначение

Назначение данного примера — показать, как сторонние средства управления безопасностью разработки можно адаптировать и интегрировать во внутреннюю программу обеспечения безопасности приложений в качестве прямого ответа на атаку.

Перечень мероприятий для обеспечения полного соответствия требованиям ИСО/МЭК 27034 (все части) может включать в себя:

а) обновление сторонних средств управления безопасностью разработки с учетом структуры МОБП:

1) обновление средств управления для обеспечения безопасности МОБП,

2) обновление средств управления безопасностью в соответствии с процедурой верификации МОБП;

b) сопоставление процедур разработки программного обеспечения с ЭМЖЦБП.

В этом примере использования описан только начальный шаг по внедрению МОБП, соответствующих ИСО/МЭК 27034, в процедуры разработки организации.

5.6.3 Контекст

В 2008 году сайты крупной компании из Соединенных Штатов подверглись атакам, что привело к небольшому повреждению внутренней базы данных. Что еще более важно, в результате взлома ботнет получил платформу для распространения вредоносных программ среди ничего не подозревающих пользователей сети Интернет.

После обнаружения взлома и выявления кода ботнета компания немедленно исправила веб-код и начала процесс по изменению внутренней культуры разработки приложений, затянувшийся на год. В течение нескольких дней ИТ-директор компании проводил встречи с ИТ-менеджерами всех подразделений, а затем разработал план по обеспечению безопасности программного кода компании. После долгих обсуждений было принято решение, что внутренняя команда опытных программистов будет более эффективной при разработке решений за счет глубокого знания компании и достаточных, по их мнению, знаний процедур написания безопасного кода.

Для решения проблемы уязвимого кода была привлечена команда лучших разработчиков и специалистов компании по компьютерной безопасности. На эту команду по безопасной разработке была возложена ответственность за составление новых процедур, обеспечивающих проактивную защиту всего написанного кода. Новые участники команды по безопасной разработке владели несколькими языками программирования и методологиями веб-разработки, администрирования баз данных и обеспечения компьютерной безопасности. Все участники считались лучшими в компании по своей специальности и были осведомлены о защите кода.

ИТ-директор поручил команде разработать рекомендации для новых процессов, способных обеспечить максимально высокую безопасность исходного кода. Группа также должна была определить инструментальные средства, необходимые разработчикам в работе, порекомендовать, как реализовать новые процессы написания безопасного кода, определить необходимость в обучении и устранить все критические уязвимости кода в течение одного года.

Разработанный процесс используется компанией практически без изменений даже спустя пять лет.

5.6.4 Этап подготовки (1.00)

На этапе подготовки был организован процесс безопасной разработки, разработчики изучили методы написания безопасного кода, были приобретены инструментальные средства для выявления уязвимостей кода, созданы возможности для совместного безопасного программирования, опубликованы стандарты безопасной разработки и политика написания безопасного кода, а также разработаны метрики для измерения уровня защиты кода.

Таблица 9 — Мероприятия по внедрению МОБП и результаты этапа подготовки

Этап подготовки	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
1.10 Административные средства управления	1.11 Создана и доведена до сведения всех разработчиков политика безопасной разработки	Опубликована политика безопасной разработки. Проверен уровень понимания политики и эффективности ее реализации	ИТ-директор. Команда по безопасной разработке. Служба безопасности. ИТ-менеджеры
	1.12 Для обеспечения соответствия стандартам безопасной разработки к ежегодным оценкам эффективности работы каждого лица, участвующего в разработке, были добавлены персональные цели	В формы оценки эффективности работы персонала была добавлена новая персональная цель для обеспечения соответствия SDL[1)]. В оценку персонала был включен пункт о соблюдении стандартов безопасной разработки	ИТ-директор. ИТ-менеджеры. Руководители команд. Разработчики

[1)] Жизненный цикл безопасной разработки (SDL).

Продолжение таблицы 9

Этап подготовки	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
	1.13 Были приобретены и установлены инструментальные средства для поиска уязвимостей в коде	Установка и обучение команды по безопасной разработке были завершены и задокументированы до проведения общего обучения в ИТ-отделе	ИТ-директор. Команда по безопасной разработке. Администраторы. Отдел поставок. Отдел сетевой инфраструктуры
	1.14 Каждый разработчик получил краткий перечень (QR) — лист (двусторонний, ламинированный, удобного формата) стандартов безопасной разработки организации и рекомендаций по написанию кода от сторонних организаций, например OWASP	Создан перечень стандартов (QR) и рекомендаций. Перечень опубликован и заламинирован. Перечень предоставлен разработчикам. Периодически проверяется наличие у разработчиков соответствующих перечней, доступных для ознакомления во время работы	Команда по безопасной разработке. Издательский отдел организации. ИТ-директор. Служба безопасности
	1.15 Разработаны метрики по измерению прогресса в ходе устранения уязвимостей кода	Номера уязвимостей, выявленных утилитами для сканирования кода, нанесены на диаграмму. ИТ-директор и менеджеры по разработке провели документированный обзор и утверждение метрик. Уязвимости, выявленные утилитами для сканирования, публикуются еженедельно и ежемесячно	Служба безопасности. Команда по безопасной разработке. ИТ-директор. Менеджеры по разработке
	1.16 Для централизованного хранения стандартов, учебных материалов, протоколов собраний команды по безопасной разработке, отчетов о метриках и обмена сведениями о технологиях обеспечения безопасности создан портал по безопасной разработке	Создан портал для обмена сведениями о безопасной разработке. На портале по безопасной разработке размещаются актуальные версии стандартов, протоколов совещаний группы по безопасной разработке, учебных материалов, рекомендаций по безопасной разработке, процедур совместного использования безопасных методов разработки и отчетов о метриках	Команда по безопасной разработке. Менеджеры по разработке. Руководители команд. Разработчики
	1.17 Разработана внутренняя программа обучения для всех разработчиков	Запланированы обучающие презентации длительностью не менее 3 ч. Запланировано обучение всех разработчиков на различных ИТ-площадках	Команда по безопасной разработке. ИТ-директор

Продолжение таблицы 9

Этап подготовки	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
	1.18 Пройдено обучение у сторонних экспертов по безопасной разработке веб-сайтов	Выбран поставщик. Запланировано и проведено трехдневное интенсивное обучение для веб-разработчиков	Команда по безопасной разработке. ИТ-директор. Отдел поставок. Разработчики. Руководители команд. Менеджеры по разработке
Обучение. Все участники команды разработчиков программного обеспечения прошли соответствующее обучение методам безопасной разработки	1.21 Основные понятия Команда по безопасной разработке создала трехчасовую базовую программу обучения безопасности для всего персонала, связанного с разработкой. Предполагается, что каждый технический специалист проектной команды хорошо знаком с концепциями, изложенными в следующих подразделах. Безопасное проектирование: - уменьшение поверхности атаки; - углубленная защита; принцип минимума полномочий; - безопасные значения по умолчанию; - модель позитивной безопасности. Моделирование угроз: - обзор моделирования угроз; - разработка, написание кода и тестирование с учетом моделей угроз. Темы по написанию безопасного кода: - десять самых распространенных уязвимостей OWASP; - ошибки в целочисленной арифметике; переполнение буфера; проблемы с управляемым кодом (Microsoft. NET/Java). Темы по тестированию безопасности: - тестирование безопасности и функциональное тестирование; - оценка рисков; методики испытаний; - автоматизация испытаний. Темы по обеспечению конфиденциальности: - типы конфиденциальных данных;	Прохождение обучения отслеживается в ИТ-отделе или в учебном отделе компании. Достигнуто стопроцентное посещение персоналом всех тренингов. Для разработчиков, которые не смогли пройти запланированное обучение, были проведены дополнительные занятия. Веб-разработчики прошли обязательное дополнительное обучение по безопасной разработке веб-сайтов	Команда по безопасной разработке. Менеджеры по разработке. Руководители команд. Разработчики

Продолжение таблицы 9

Этап подготовки	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
	- эффективные методики конфиденциального проектирования; - анализ рисков; - эффективные методики конфиденциальной разработки; - эффективные методики конфиденциального тестирования		
	1.22 Обучение запуску утилиты для сканирования кода и анализу результатов	Зафиксирована стопроцентная посещаемость занятий. Для разработчиков, которые не смогли пройти запланированное обучение, были проведены дополнительные занятия. Завершено обучение по использованию утилиты для сканирования кода и анализу результатов ее работы	Команда по безопасной разработке. Менеджеры по разработке. Руководители команд. Разработчики
	1.23 Усовершенствованные концепции безопасности: было рекомендовано проведение дополнительного обучения по следующим аспектам: - безопасное проектирование и архитектура; - создание пользовательского интерфейса; - подробное изучение ошибок безопасности; - процедуры реагирования на нарушение безопасности; - внедрение специализированной защиты от угроз	Прохождение обучения отслеживается в ИТ-отделе или в учебном отделе компании. Посещение персоналом обучения отмечается в личных делах	Менеджеры по разработке. Руководители команд. Разработчики
	1.24 Повышение квалификации Для ознакомления с методами написания безопасного кода каждый разработчик обязан пройти не менее одного учебного курса в год	Прохождение обучения отслеживается в ИТ-отделе или в учебном отделе компании. Посещение персоналом обучения отмечается в личных делах	Менеджеры по разработке. Руководители команд. Разработчики
	1.25 Самостоятельное обучение. Разработчикам рекомендуется ознакомиться со следующими публикациями (из различных дисциплин): - Writing Secure Code, Version 2 (ISBN:0-7356-1722-8);	Прохождение обучения отслеживается в ИТ-отделе или в учебном отделе компании. Посещение персоналом обучения отмечается в личных делах	Менеджеры по разработке. Руководители команд. Разработчики

Окончание таблицы 9

Этап подготовки	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
	- последняя версия руководства OWASP для разработчиков (http://www.owasp.org/index.php/Category:OWASP Guide Project); - OWASP Top Ten (http://www.owasp.org/index.php/Category:OWASP Top Ten Project)		

5.6.5 Этап составления требований (2.00)

Учет вопросов безопасности с самого начала разработки является фундаментальным принципом создания безопасных систем. Хотя во многих проектах разработки «следующие версии" программного обеспечения основаны на предыдущих, этап составления требований и первоначального планирования нового выпуска или версии позволяет создавать наиболее защищенное программное обеспечение.

На этапе составления требований компания может оценить, как требования к обеспечению безопасности будут интегрироваться в процесс разработки, определить ключевые цели по обеспечению безопасности и повысить безопасность программного обеспечения при минимальном нарушении планов и графиков. При этом также рассматривается, как функции и мероприятия по обеспечению безопасности программного обеспечения будут взаимодействовать с другим программным обеспечением. (Это является решающим фактором для удовлетворения потребностей пользователей в ходе интеграции отдельных продуктов в безопасные системы.)

Хотя часть требований к функциям безопасности составляется на основе моделирования угроз, запросы клиентов могут играть важную роль в составлении таких требований. Кроме того, некоторые требования обусловлены необходимостью соблюдения отраслевых стандартов или правил и должны входить в обычный процесс планирования.

Таблица 10 — Мероприятия по внедрению МОБП и результаты этапа составления требований

Этап составления требований	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
2.10 Первоначальная оценка рисков безопасности	2.11 Первоначальная оценка рисков безопасности: разработчик составляет оценку рисков и должен обосновать все несанкционированные изменения параметров и настроек безопасности. Вопросы по установке: изменялись ли параметры операционной системы или списки контроля доступа? Вопросы о поверхности атак: используются ли в коде повышенные привилегии или подключение к Интернету? Вопросы по коду мобильных приложений: написан ли код с использованием продвинутых технологий безопасности, таких как .NET или Java? Используются ли средства управления ActiveX?	Составлена документация, подтверждающая факт проверки уровня безопасности каждого метода и свойства каждого средства управления ActiveX. Была составлена формальная модель угрозы для следующих ситуаций: - приложение имеет сетевой интерфейс; - приложение поддерживает взаимодействие в режиме ядра и режиме пользователя; - пользователи без прав администратора взаимодействуют с процессами с более высокими привилегиями; - приложение является функцией безопасности другого кода	Менеджеры по разработке. Руководители команд. Разработчики

Окончание таблицы 10

Этап составления требований	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
	Функция безопасности: использует ли код существующие механизмы безопасности или содержит собственные средства безопасности? Используется ли криптография?		
2.2 Уровень конфиденциальности	2.21 Типы конфиденциальных данных: - анонимные; - персональные данные, ПДн; - персональные данные с ограниченным доступом	Составлен анализ типов данных, которые будут обрабатываться кодом. Установлен и задокументирован порог/уровень конфиденциальности	Руководители команд. Разработчики. Служба безопасности
	2.2 Компоненты с наивысшим уровнем конфиденциальности были подвергнуты тщательному анализу, зачастую с привлечением экспертов по конфиденциальности. Цель анализа: убедиться, что приложение не допускает утечки персональных данных и не нарушает законов или положений о конфиденциальности	Разработана документация с результатами анализа уровней конфиденциальности каждой программы и модуля при условии превышения порога конфиденциальности из 2.21	Руководители команд. Разработчики. Служба безопасности

5.6.6 Этап проектирования (3.00)

На этапе проектирования определяются общие требования к программному обеспечению и его структура. Этап проектирования является наиболее важным этапом всего процесса безопасной разработки, поскольку именно на нем определяется уровень безопасности разработки ПО[1)]. С точки зрения безопасности ключевыми элементами этапа проектирования являются: определение архитектуры безопасности и руководящих принципов проектирования; документирование поверхности атаки программного обеспечения; моделирование угроз. Все мероприятия на этапе проектирования вносятся в постоянную документацию компьютерной системы.

1) Определение архитектуры безопасности и руководящих принципов проектирования. Необходимо определить общую структуру ПО с точки зрения безопасности и выделить те компоненты, правильное функционирование которых имеет важное значение для безопасности. Кроме того, следует сформировать общие методы проектирования ПО: например, многоуровневая структура (деление ПО на четко определенные компоненты, структура которых позволяет избежать циклической взаимозависимости), использование строго типизированного языка и наименьшего количества привилегий, а также уменьшение поверхности атаки. Специфика отдельных элементов архитектуры будет подробно описана в отдельных спецификациях проекта, но архитектура безопасности определяет общий взгляд на принципы ее обеспечения.

2) Документация поверхности атаки на ПО. Учитывая, что обеспечить идеальную безопасность ПО невозможно, важно, чтобы всем пользователям по умолчанию были доступны только функции, которые будут использоваться подавляющим большинством пользователей, и чтобы эти функции имели минимально возможный уровень привилегий. Благодаря отслеживанию поверхности атаки команды разработчиков получают постоянно обновляемые показатели уровня безопасности по умолчанию и могут обнаруживать случаи, когда ПО становится более уязвимым для атак.

3) Моделирование угроз. Эта процедура проводится на уровне компонентов. Активы, которыми должно управлять ПО, и интерфейсы, с помощью которых можно получить доступ к таким активам,

[1)] Программное обеспечение.

моделируются с целью выявления угроз, которые могут нанести им вред, а также определения вероятности нанесения такого вреда (оценка рисков). При этом составляются снижающие риски контрмеры в форме функций безопасности, например шифрования, либо в форме строго контролируемых функций ПО, защищающих активы.

Таблица 11 — Мероприятия по внедрению МОБП и результаты этапа проектирования

Этап проектирования	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
3.10 Определение архитектуры безопасности	3.11 Принципы безопасного проектирования: - модель позитивной безопасности (белый список разрешенных действий); - минимизация поверхности атаки (и входных точек); - классификация активов (защита того, что используется); - защита по умолчанию (обеспечение защиты во время всего процесса работы с ПО); - принцип наименьших привилегий (для любых действий с кодом); - углубленная защита (различные средства управления не позволяют использовать уязвимости); - безопасный сбой (последовательность действий при сбое запрещает использование ПО); - принцип «безопасность через неясность" не используется, так как на самом деле не обеспечивает безопасности. 3.12 Разделение обязанностей (системные администраторы могут устанавливать политики в коде, но не могут входить в пользовательский интерфейс с правами администратора). 3.13 Ограничение внешнего воздействия: - разделение по зонам (для ограничения возможных повреждений в случае сбоя); - разделение привилегий (отдельные сеансы пользователей из зон с повышенными правами доступа); - проверка входных данных (определение приемлемого формата и диапазона данных и реакции на некорректные данные)	Составлена документация, подтверждающая факт проведения анализа архитектуры безопасности на начальном этапе проектирования. Задокументировано соблюдение стандартов безопасной разработки на этапе проектирования	Руководители команд. Разработчики. Менеджеры по разработке

Окончание таблицы 11

Этап проектирования	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
3.20 Моделирование рисков угроз/схемы потоков данных	3.21 Определение объектов, которые необходимо защитить: - персональные данные; - соответствие требованиям; - репутация; - финансовые показатели; - соглашение об уровне обслуживания; - конфиденциальность. 3.22 Обзор приложения: - компоненты; - потоки данных; - границы уровней доверия приложений. 3.23 Составление обзора приложения: - составление полного сценария развертывания; - определение технологий (серверы, базы данных, веб-интерфейсы); - определение механизмов обеспечения безопасности приложений. 3.24 Разбор приложения: - определение границ уровней доверия приложений; - определение потоков данных; - определение точек входа; - определение точек выхода. 3.25 Использование рейтинга риска угроз (STRIDE): - подделка персональных данных: пользователи не могут выступать в качестве другого пользователя; - искажение данных: пользователи могут изменять любые полученные данные. Приложение должно тщательно проверять все полученные от пользователя данные на предмет искажения; - отказ от действий: приложение должно иметь надлежащие средства отслеживания действий, например журналы доступа и транзакций; - раскрытие информации: приложения должны иметь строгие средства управления, чтобы предотвратить подделку идентификаторов пользователей и минимизировать объем информации, хранящейся в браузере; - отказ в обслуживании: приложения должны минимизировать возможность проведения атак типа «отказ в обслуживании"; - каждый фасет приложения должен выполнять как можно меньший объем работы; - несанкционированное повышение привилегий: все действия должны проходить через матрицу авторизации, чтобы доступ к привилегированным функциям могли получать только правильные роли	Составлены программные и командные документы, подтверждающие факт проведения анализа архитектуры безопасности на этапе проектирования. Руководители групп и менеджеры по разработке подтвердили, что в проекте соблюдены стандарты безопасной разработки	Руководители команд. Разработчики. Менеджеры по разработке

5.6.7 Этап реализации (4.00)

На этапе реализации команда разработчиков пишет код, тестирует и интегрирует программное обеспечение. Здесь эффективно внедряются шаги, предпринятые для устранения недостатков или предотвращения их первоначального появления. Такие шаги значительно снижают вероятность того, что уязвимости попадут в окончательную версию ПО, выпущенную для пользователей. Результаты моделирования угроз содержат наиболее важные для этапа реализации сведения. Разработчики уделяют особое внимание анализу исходного кода, который устраняет высокоприоритетные угрозы, а также проводят тестирования, направленные на блокировку или смягчение последствий таких угроз.

Элементы SDL, которые используются на этапе реализации:

1) Внедрение стандартов написания и тестирования кода. Стандарты написания кода помогли разработчикам избежать ошибок, которые могли привести к появлению уязвимостей. Например, использование более безопасных и согласованных процедур обработки строк и операций с буфером поможет избежать риска переполнения буфера. Стандарты и эффективные методики тестирования позволяют гарантировать, что тестирование направлено на выявление потенциальных уязвимостей, а не на проверку правильной работы программных функций.

2) Применение инструментальных средств для выполнияя фаззинг-тестирования. В ходе фаззинга в программные интерфейсы приложений (API) и сетевые интерфейсы вводятся структурированные, но недействительные входные данные, которые позволяют максимизировать вероятность обнаружения ошибок, открывающих уязвимости ПО.

3) Применение инструментальных средств для статического анализа кода. Инструментальные средства могут обнаружить некоторые виды недостатков кода, которые приводят к уязвимостям, включая переполнения буфера, целочисленные переполнения и неинициализированные переменные.

4) Проведение экспертизы исходного кода. Экспертиза исходного кода, в ходе которой специально обученные разработчики изучают исходный код, выявляют и устраняют потенциальные уязвимости, дополняет собой автоматизированные инструментальные средства и тесты. Она является важным этапом процесса устранения уязвимостей ПО в ходе разработки.

Таблица 12 — Мероприятия по внедрению МОБП и результаты этапа реализации

Этап реализации	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
4.10 Подготовка кода и проверка безопасности	4.11 Применение внутренних стандартов безопасной разработки: - анализ нового исходного кода на предмет уязвимостей; - исправление всех выявленных недостатков; - проведение подробного моделирования угроз; - экспертная оценка кода; - привлечение разработчиков для частого анализа нового исходного кода на наличие уязвимостей (даже по нескольку раз в день) и их исправление на начальном этапе разработки; - отслеживание всех действий с данными, которые использует код.	Частый анализ исходного кода в процессе написания с помощью утилиты для поиска уязвимостей. Составление еженедельных отчетов с помощью утилиты для поиска уязвимостей, подтверждающих выполнение анализа. Контроль версий для отслеживания исправления уязвимостей при последующих анализах	Руководители команд. Разработчики. Менеджеры по разработке

Продолжение таблицы 12

Этап реализации	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
	4.12 Тестирование модулей кода с помощью утилиты для поиска уязвимостей	С целью обновления электронной таблицы метрик отдел безопасности должен получать еженедельные и ежемесячные отчеты от утилиты для поиска уязвимостей. Ведение метрик для отслеживания уязвимостей на основании еженедельных отчетов. Документирование результатов поиска опасных уязвимостей и ведение графиков для наглядного отображения прогресса	Служба безопасности. ИТ-директор. Руководители команд. Разработчики. Менеджеры по разработке
4.2 Безопасность базы данных	4.21 Общая безопасность. Администраторы базы данных несут полную ответственность за схему и структуру. Для доступа к любым данным в базе требуются идентифицируемые учетные записи пользователей. Транзакции, добавляющие данные в базу или изменяющие их, должны выполняться только с помощью авторизованной функции программы. Все транзакции и действия в базе данных должны вноситься в журналы аудита	Разработана документация, которая подтверждает, что взаимодействовать с данными в базе могут только идентифицируемые учетные записи пользователей. Разработана документация, которая подтверждает, что администраторы баз данных не могут изменять или удалять данные. Разработана документация, которая подтверждает, что только администраторы баз данных могут создавать или изменять схему базы данных. Представлено подтверждение того, что все изменения и просмотры данных в базе записываются. Представлено подтверждение того, что файл журнала базы данных защищен от изменения и хранится в месте, к которому не могут получить доступа администраторы базы данных и разработчики	Администраторы базы данных. Администраторы учетных записей пользователей. Руководители команд. Разработчики. Менеджеры по разработке. Служба безопасности
	4.22 Защита паролем. Для обращения с паролями учетных записей обычных и служебных пользователей будет использоваться система аутентификации учетных записей пользователей. Срок действия паролей служебных учетных записей (используемых программным кодом только без возможности локального входа) истекает ежегодно.	Составлена документация, согласно которой доступ к данным в базе имеют только учетные записи пользователей. Составлена документация по всем правам и настройкам служебных учетных записей. Составлена документация, подтверждающая, что все учетные записи соответствуют правилам истечения срока действия пароля	Администраторы базы данных. Администраторы учетных записей пользователей. Руководители команд. Разработчики. Менеджеры по разработке. Служба безопасности

Окончание таблицы 12

Этап реализации	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
	Учетные записи пользователей базы данных истекают через 45 дней после синхронизации с системой аутентификации учетных записей пользователей и учетными записями других служб		
	4.23 Учетные записи Администратор раздела пользователей управляет учетными записями, имеющими доступ к базам данных. Программистам запрещено использовать универсальные учетные записи для доступа к базам данных. Поскольку прямой доступ к базе данных запрещен, необходимо использовать хранимые процедуры. Чтобы избежать возникновения уязвимостей при внедрении SQL, необходимо использовать переменные связывания	Составлена документация, согласно которой получить доступ к данным в базе данных могут только учетные записи пользователей, которые используют программные транзакции. Составлена документация по всем правам и настройкам служебных учетных записей. Составлена документация, согласно которой прямой доступ к данным невозможен и требуется использование хранимых процедур	Администраторы базы данных. Администраторы учетных записей пользователей. Руководители команд. Менеджеры по разработке. Разработчики. Менеджеры по разработке. Служба безопасности

5.6.8 Этап верификации (5.00)

Этап верификации — это точка, в которой приложение функционально готово, переходит к этапу функционального бета-тестирования пользователями и проходит дополнительные предпроизводственные проверки безопасности. Когда приложение проходит бета-тестирование на этом этапе, команда выполняет интенсивное тестирование безопасности продукта, в которое входят дополнительные проверки кода, а также узконаправленное тестирование безопасности. Эффективность этого тестирования измеряется с помощью утилиты для поиска уязвимостей в исходном коде и путем проведения экспертизы исходного кода.

Важно отметить, что экспертиза и тестирование наиболее приоритетного исходного кода (исходный код, который входит в поверхность атаки приложения) имеют решающее значение для нескольких частей SDL. Например, экспертиза исходного кода и тестирование должны обязательно выполняться на этапе реализации с целью раннего выявления проблем и устранения их источников. Они также важны и на этапе верификации, когда продукт близок к выпуску.

В этом примере МОБП предназначена только для наиболее приоритетного исходного кода.

Таблица 13 — Мероприятия по внедрению МОБП и результаты этапа верификации

Этап верификации	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
5.10 Экспертиза исходного кода	5.11 Экспертная оценка: - авторизация; - контроль доступа; - проверка входных данных; - обработка ошибок; - управление сессиями; - ключи форм или частая смена сессий (на случай подделки межсайтовых запросов — CSRF-защита); - корректное ведение журналов приложения; - конфиденциальность	Представлено подтверждение того, что экспертиза исходного кода была проведена другими участниками команды помимо первоначальных разработчиков. Представлено подтверждение соблюдения стандартов безопасной разработки. Представлено подтверждение того, что в окончательной версии кода не было выявлено ОПАСНЫХ уязвимостей	Руководители команд. Разработчики. Менеджеры по разработке

Окончание таблицы 13

Этап верификации	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
5.20 Анализ транзакций	5.21 Проведение анализа транзакций: - определение всех точек входа, включая проверку входных данных из внешних источников; - путь обработки входных данных в приложении; - выходные данные, полученные в результате обработки входных; - файлы cookie или информация о состоянии, которая передается между клиентом и сервером; - динамический и статический анализ потока данных, в который входят сведения о том, где и когда установлены переменные и как они используются; - обработка ошибок; - ведение журналов/аудит; - криптографическая защита; - управление сессиями, вход в систему/выход из системы	Составлена и подтверждена документация о проведении анализа транзакций	Руководители команд. Разработчики. Менеджеры по разработке

5.6.9 Этап выпуска (6.00)

На этапе выпуска приложение должно пройти окончательную проверку безопасности (final security review, FSR). Цель FSR — ответить на вопрос: готово ли это приложение для отправки клиентам с точки зрения безопасности? FSR проводится до завершения работы над приложением и с учетом сферы его применения. FSR проходит стабильную версию приложения, а перед выпуском допускается внесение только минимальных изменений, не связанных с безопасностью.

FSR — это не просто тест, и его цель не состоит в нахождении всех оставшихся уязвимостей. Скорее, FSR позволяет команде и высшему руководству компании получить общую картину состояния безопасности ПО и понять, сможет ли оно противостоять атакам после выпуска для клиентов. Если FSR обнаруживает шаблон неустраненной уязвимости, нужно не только исправить обнаруженную уязвимость, но и вернуться к более раннему этапу разработки и выполнить определенные действия для устранения причин ее появления (например, повысить качество обучения, усовершенствовать инструментальные средства).

Таблица 14 — Мероприятия по внедрению МОБП и результаты этапа выпуска

Этап выпуска	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
6.10 Окончательная проверка безопасности (FSR)	6.11 Выводы отчета по FSR: - определение основной причины всех существенных уязвимостей; - создание модели угрозы необходимо в следующих случаях: - приложение имеет сетевой интерфейс, - приложение поддерживает взаимодействие в режиме ядра и режиме пользователя,	Составлена документация, согласно которой менеджеры по разработке проанализировали результаты FSR и функционального тестирования и одобрили выпуск. Проведена и задокументирована экспертная оценка результатов поиска уязвимостей.	Руководители команд. Разработчики. Специалист по продвижению. Менеджеры по разработке

Окончание таблицы 14

Этап выпуска	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
	- пользователи без прав администратора взаимодействуют с процессами с более высокими привилегиями, - приложение является функцией безопасности другого кода	Была повторно проверена безопасность каждого метода и свойства в каждом средстве управления ActiveX, данные об этом были задокументированы. Если код написан для нового продукта, проводится дополнительная тщательная проверка безопасности проектирования и документируются ее результаты	

5.6.10 Этап технического обеспечения, поддержки и обслуживания (7.00)

Постоянная поддержка производственных компьютерных систем необходима для удовлетворения изменяющихся нормативных изменений и потребностей пользователей, а также для периодического исправления ошибок в рамках аудита и обеспечения защиты от новых угроз. Даже если текущие обстоятельства не влияют на внесение изменений в программный код, компания составила график периодического повторного сканирования систем, чтобы гарантировать, что новые угрозы не будут представлять опасности для существующих программных продуктов. На этом этапе также устанавливается следующая цель: все лица, занятые в разработке ПО, должны расширять свои технические знания по вопросам и методам безопасности и поддерживать их актуальность.

Таблица 15 — Мероприятия по внедрению МОБП и результаты этапа поддержки и обслуживания

Этап поддержки и обслуживания	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
7.10 Проверка безопасности	7.11 Запланированный анализ производственного исходного кода. Ежеквартальные обновления утилиты для поиска уязвимостей могут обеспечить обнаружение новых уязвимостей. В соответствии с внутренним стандартом безопасной разработки необходимо проводить ежеквартальные проверки приложений, которые обрабатывают конфиденциальные персональные или финансовые данные	Ведется журнал обновления утилиты для поиска уязвимостей. Проводится и документируется необходимый ежеквартальный повторный анализ исходного кода. При внесении любых изменений в производственный код проводится новый поиск уязвимостей. Составлен аудиторский отчет с указанием обнаруженных недостатков	Служба безопасности. Команда по безопасной разработке. Руководители команд. Разработчики. Менеджеры по разработке. Специалист по продвижению
	7.12 Сторонние аудиторы. Аудиты сетевой инфраструктуры, баз данных и приложений, включая веб-приложения, проводятся не реже одного раза в год. Проводятся проверки соответствия с учетом требований SOX, NACHA и других регулирующих организаций	Для выявления необнаруженных недостатков проведено сравнение аудиторского отчета с внутренним журналом исправления уязвимостей. Задокументированы исправления и корректирующие меры по результатам аудита	Сторонние ИТ-аудиторы. Служба безопасности. ИТ-директор. Менеджеры по разработке. Руководители команд

Окончание таблицы 15

Этап поддержки и обслуживания	Мероприятия по внедрению МОБП	Полученные МОБП	Ответственные должности
	7.13 Пользовательские запросы на внесение изменений или функциональные сбои. Документирование и проверка уровня безопасности изменений функций, запрошенных пользователями. Внесение новых функций по запросам пользователей может потребовать обновления модели анализа угроз	После внесения любых изменений в производственный код необходимо проводить повторный поиск уязвимостей	Руководители команд. Разработчики. Специалист по продвижению
	7.14 Обнаружение атак. Если это технически возможно, в приложения добавлен специальный код, связывающий их с утилитой для обнаружения уязвимостей и атак, которая позволяет выявлять и пресекать атаки на работающие приложения и собирать необходимую информацию. Для выявления тенденций в информации об атаках будет установлена связь со средством мониторинга для обнаружения угроз	Необходимо предоставить подтверждение того, что соответствующий код был добавлен в производственное ПО. Необходимо предоставить подтверждение того, что мониторинг угроз приложений работает правильно	Руководители команд. Разработчики. Менеджеры по разработке. Служба безопасности
7.20 Внешние изменения	7.21 Мониторинг внешних требований или изменений. Нормативные изменения Новые работающие на практике критические уязвимости, которые потенциально затронут код компании	Необходимо представить подтверждение того, что для выявления внешних изменений, которые могут повлиять на уровень поддержки, и (или) новых требований по безопасности налажен соответствующий канал связи	ИТ-директор. Менеджеры по разработке. Служба безопасности. Бизнес-пользователи. Юридический отдел
7.30 Поддержание знаний в области безопасности	7.31 Повышение квалификации. Для ознакомления с методами написания безопасного кода и новыми угрозами каждый разработчик обязан пройти не менее одного учебного курса в год	Прохождение обучения отслеживается в ИТ-отделе или в учебном отделе компании. Посещение персоналом обучения отмечено в личных делах	Менеджеры по разработке. Руководители команд. Разработчики

Приложение А
(справочное)

Примеры использования из 5.2 на языке XML

Примеры приведены с целью упрощения разработки и передачи данных МОБП внутри организации или между разными организациями с учетом требований ИСО/МЭК 27034-5-1.

Таблица А.1 — XML-пример названия МОБП, написанного на трех языках

```
<?xml version="1.0" encoding="UTF-8"?>
<asc:asc-package xmlns:asc="http://iso.org/ISO27034/ASC-structure" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xml-asc-package-schema-version="1.0.0.0">
<asc:package-content>
    <asc:package-identification>
        <!-- Content removed for simplification -->
    </asc:package-identification>
    <asc:asc xml-asc-schema-version="1.0.0.0">
        <asc:content>
        <asc:identification>
        <asc:uid>ORGANIsation-ASD-042</asc:uid>
        <asc:name>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Code Review</asc:text>
            </asc:localized-information>
            <asc:localized-information language="FR" country="CA" organization="ORGANIsation">
                <asc:text>Révision de code</asc:text>
            </asc:localized-information>
        <asc:localized-information language="RU" country="RU" organization="ORGANIsation">
            <asc:text>Анализ кода</asc:text>
        </asc:localized-information>
    </asc:name>
<!-- Content removed for simplification -->

</asc:asc-package>
```

Таблица А.2 — XML-пример процедуры утверждения МОБП и соответствующих подписей

```
<?xml version="1.0" encoding="UTF-8"?>
<asc:asc-package xmlns:asc="http://iso.org/ISO27034/ASC-structure" xmlns:xsi="http://www.w3.org/2001/XMLSche-
ma-instance" xml-asc-package-schema-version="1.0.0.0">
    <asc:package-content>
        <asc:package-identification>
            <!-- Содержание удалено для упрощения текста документа -->
        </asc:package-identification>
        <asc:asc xml-asc-schema-version="1.0.0.0">
            <asc:content>
                <asc:identification>
                    <asc:uid>ORGANIsation-ASD-042</asc:uid>
                    <asc:name>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                            <asc:text>Code Review</asc:text>
                        </asc:localized-information>
                    </asc:name>
                    <asc:version number="1.3.6.0" date="2016-01-04" life-cycle-stage="ACTIVE"></asc:version>
                    <!-- Content removed for simplification -->
                </asc:identification>
```

Продолжение таблицы А.2

```
            <asc:objective>
                <!-- Content removed for simplification -->
            </asc:objective>
            <asc:security-activity>
                <!-- Content removed for simplification -->
            </asc:security-activity>
            <asc:verification-measurement>
                <!-- Content removed for simplification -->
            </asc:verification-measurement>
        </asc:content>
        <asc:approval-e-signatures>
            <asc:approval-stage>
                <asc:date>2011-09-23</asc:date>
                <asc:approval-stage-type>CREATION_REQUEST</asc:approval-stage-type>
                <asc:approver>
                    <asc:name>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                            <asc:text>Herbert George Wells</asc:text>
                        </asc:localized-information>
                    </asc:name>
                    <asc:coordinate location-name="Office">
                        <asc:organization>
                            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                                <asc:text>ORGANIsation inc.</asc:text>
                            </asc:localized-information>
                        </asc:organization>
                        <asc:department>
                            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                                <asc:text>Application Security Department</asc:text>
                            </asc:localized-information>
                        </asc:department>
                        <asc:emails>
                            <asc:email type="Office">JVernes@ORGANIsation.com</asc:email>
                        </asc:emails>
                        <asc:country>
                            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                                <asc:text>Canada</asc:text>
                            </asc:localized-information>
                        </asc:country>
                    </asc:coordinate>
                </asc:approver>
                <asc:approver-e-signature>
                    <asc:e-signature-param>HGWells@ORGANIsation.com</asc:e-signature-param>
                    <asc:e-signature-param>Version: PGP Universal 3.2.0 (Build 1950)</asc:e-signature-param>
                    <asc:e-signature-param>Charset: us-ascii</asc:e-signature-param>
                    <asc:e-signature-data>wsBVAwUBT06tfp/JsGz ... fwymKISR63wb7QQ===x0gO</asc:e-signature-data>
                </asc:approver-e-signature>
            </asc:approval-stage>
            <asc:approval-stage>
            <asc:date>2012-01-11</asc:date>
            <asc:approval-stage-type>VALIDATION</asc:approval-stage-type>
                <asc:approver>
                    <asc:name>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
```

Продолжение таблицы А.2

```
                        <asc:text>Arthur C. Clarke</asc:text>
                    </asc:localized-information>
                </asc:name>
                <asc:coordinate location-name="Office">
                    <asc:organization>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                            <asc:text>ORGANIsation inc.</asc:text>
                        </asc:localized-information>
                    </asc:organization>
                    <asc:department>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                            <asc:text>Application Security Department</asc:text>
                        </asc:localized-information>
                    </asc:department>
                    <asc:emails>
                        <asc:email type="Office">ACClarke@ORGANIsation.com</asc:email>
                    </asc:emails>
                    <asc:country>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                            <asc:text>Canada</asc:text>
                        </asc:localized-information>
                    </asc:country>
                </asc:coordinate>
            </asc:approver>
        </asc:approval-stage>
        <asc:approval-stage>
        <asc:date>2012-05-10</asc:date>
        <asc:approval-stage-type>DEVELOPMENT</asc:approval-stage-type>
            <asc:approver>
                <asc:name>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Frank Herbert</asc:text>
                    </asc:localized-information>
                </asc:name>
                <asc:coordinate location-name="Office">
                    <asc:organization>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                            <asc:text>ORGANIsation inc.</asc:text>
                        </asc:localized-information>
                    </asc:organization>
                    <asc:department>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                            <asc:text>Application Security Department</asc:text>
                        </asc:localized-information>
                    </asc:department>
                    <asc:emails>
                        <asc:email type="Office">FHerbert@ORGANIsation.com</asc:email>
                    </asc:emails>
                    <asc:country>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                            <asc:text>Canada</asc:text>
                        </asc:localized-information>
                    </asc:country>
                </asc:coordinate>
```

Продолжение таблицы А.2

```
            </asc:approver>
        </asc:approval-stage>
        <asc:approval-stage>
        <asc:date>2012-09-07</asc:date>
        <asc:approval-stage-type>VERIFICATION</asc:approval-stage-type>
            <asc:approver>
                <asc:name>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Ray Bradbury</asc:text>
                    </asc:localized-information>
                </asc:name>
                <asc:coordinate location-name="Office">
                <asc:organization>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>ORGANIsation inc.</asc:text>
                    </asc:localized-information>
                </asc:organization>
                <asc:department>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Application Security Department</asc:text>
                    </asc:localized-information>
                </asc:department>
                <asc:emails>
                    <asc:email type="Office">RBradbury@ORGANIsation.com</asc:email>
                </asc:emails>
                <asc:country>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Canada</asc:text>
                    </asc:localized-information>
                </asc:country>
            </asc:approver>
        </asc:approval-stage>
        <asc:approval-stage>
        <asc:date>2012-09-17</asc:date>
            <asc:approver>
                <asc:name>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>William Gibson</asc:text>
                    </asc:localized-information>
                </asc:name>
                <asc:organization>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>ORGANIsation inc.</asc:text>
                        <asc:text>ORGANIsation inc.</asc:text>
                    </asc:localized-information>
                </asc:organization>
                <asc:department>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Application Security Department</asc:text>
                    </asc:localized-information>
                </asc:department>
                <asc:emails>
                    <asc:email type="Office">WGibson@ORGANIsation.com</asc:email>
                </asc:emails>
```

Продолжение таблицы А.2

```
            <asc:country>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Canada</asc:text>
                </asc:localized-information>
            </asc:country>
            </asc:coordinate>
        </asc:approver>
    </asc:approval-stage>
    <asc:approval-stage>
    <asc:date>2012-10-07</asc:date>
    <asc:approval-stage-type>APPROVAL</asc:approval-stage-type>
        <asc:approver>
            <asc:name>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>Robert Heinlein</asc:text>
                </asc:localized-information>
            </asc:name>
            <asc:coordinate location-name="Office">
                <asc:organization>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>ORGANIsation inc.</asc:text>
                    </asc:localized-information>
                </asc:organization>
                <asc:department>
                    <asc:text>Application Security Department</asc:text>
                    </asc:localized-information>
                </asc:department>
                <asc:emails>
                    <asc:email type="Office">RHeinlein@ORGANIsation.com</asc:email>
                </asc:emails>
                <asc:country>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Canada</asc:text>
                    </asc:localized-information>
                </asc:country>
            </asc:coordinate>
        </asc:approver>
        <asc:approver-e-signature>
            <asc:e-signature-param>RHeinlein@ORGANIsation.com</asc:e-signature-param>
            <asc:e-signature-param>Version: PGP Universal 3.2.0 (Build 1950)</asc:e-signature-param>
            <asc:e-signature-param>Charset: us-ascii</asc:e-signature-param>
            <asc:e-signature-data> Gz86uwqAQgcAp3fe ... B45vjfqO4Vq/woF</asc:e-signature-data>
        </asc:approver-e-signature>
    </asc:approval-stage>
    <asc:approval-stage>
    <asc:date>2012-10-17</asc:date>
    <asc:approval-stage-type>OWNERS_FINAL_APPROVAL</asc:approval-stage-type>
        <asc:approver>
            <asc:name>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>Douglas Adams</asc:text>
                </asc:localized-information>
            </asc:name>
            <asc:coordinate location-name="Office">
```

Продолжение таблицы А.2

```
                <asc:organization>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>ORGANIsation inc.</asc:text>
                    </asc:localized-information>
                </asc:organization>
                <asc:department>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Application Security Department</asc:text>
                    </asc:localized-information>
                </asc:department>
                <asc:emails>
                    <asc:email type="Office">DAdams@ORGANIsation.com</asc:email>
                </asc:emails>
                <asc:country>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Canada</asc:text>
                    </asc:localized-information>
                </asc:country>
            </asc:coordinate>
        </asc:approver>
        <asc:approver-e-signature>
            <asc:e-signature-param>DAdams@ORGANIsation.com</asc:e-signature-param>
            <asc:e-signature-param>Version: PGP Universal 3.2.0 (Build 1950)</asc:e-signature-param>
            <asc:e-signature-param>Charset: us-ascii</asc:e-signature-param>
            <asc:e-signature-data>bgHi0LLo+OyTx9T4uGCyx ... A09CKT4alsmvtOFLvtuB</asc:e-signature-data>
        </asc:approver-e-signature>
    </asc:approval-stage>
    <asc:approval-stage>
    <asc:date>2012-11-06</asc:date>
    <asc:approval-stage-type>PUBLISHED_FOR_TRAINING</asc:approval-stage-type>
        <asc:approver>
            <asc:name>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>Isaac Asimov</asc:text>
                </asc:localized-information>
            </asc:name>
            <asc:coordinate location-name="Office">
                <asc:organization>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>ORGANIsation inc.</asc:text>
                    </asc:localized-information>
                </asc:organization>
                <asc:department>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Application Security Department</asc:text>
                    </asc:localized-information>
                </asc:department>
                <asc:emails>
                    <asc:email type="Office">IAsimov@ORGANIsation.com</asc:email>
                </asc:emails>
                <asc:country>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Canada</asc:text>
```

Окончание таблицы А.2

```
                                </asc:localized-information>
                            </asc:country>
                        </asc:coordinate>
                    </asc:approver>
                </asc:approval-stage>
                <asc:approval-stage>
                <asc:date>2013-03-06</asc:date>
                <asc:approval-stage-type>ACTIVE</asc:approval-stage-type>
                <asc:approver>
                    <asc:name>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Mary Shelley</asc:text>
                        </asc:localized-information>
                    </asc:name>
                        <asc:text>ORGANIsation inc.</asc:text>
                        </asc:localized-information>
                    </asc:organization>
                    <asc:department>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Application Security Department</asc:text>
                        </asc:localized-information>
                    </asc:department>
                    <asc:emails>
                        <asc:email type="Office">MShelley@ORGANIsation.com</asc:email>
                    </asc:emails>
                    <asc:country>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Canada</asc:text>
                        </asc:localized-information>
                    </asc:country>
                    </asc:coordinate>
                </asc:approver>
            </asc:approval-stage>
        </asc:approval-e-signatures>
    </asc:asc>
</asc:package-content>
<asc:package-editor-e-signature>
<!-- Content removed for simplification -->
</asc:package-editor-e-signature>
</asc:asc-package>
```

Таблица А.3 — XML-пример определения дочерней МОБП

```
<?xml version="1.0" encoding="UTF-8"?>
<asc:asc-package  xmlns:asc="http://iso.org/ISO27034/ASC-structure"  xmlns:x-si="http://www.w3.org/2001/XMLSchema-instance"
xml-asc-package-schema-version="1.0.0.0">
<asc:package-content>
    <asc:package-identification>
        <!-- Content removed for simplification -->
    </asc:package-identification>
    <asc:asc xml-asc-schema-version="1.0.0.0">
        <asc:content>
            <asc:identification>
                <asc:uid>ORGANIsation-ASD-042</asc:uid>
```

Продолжение таблицы А.3

```
            <asc:name>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>Code Review</asc:text>
                </asc:localized-information>
            <asc:version number="1.3.6.0" date="2016-01-04" life-cycle-stage="ACTIVE"></asc:version>
            <asc:date>2016-01-04</asc:date>
            <asc:description>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>This ASC is used to help developers to perform a code review control for JAVA applica-
                    tions. </asc:text>
                </asc:localized-information>
            </asc:description>
            <asc:children>
                <asc:child>
                    <asc:ref-asc>ORGANIsation-ASD-043</asc:ref-asc>
                    <asc:description>
                        <asc:text>Code Classification</asc:text>
                        </asc:localized-information>
                    </asc:description>
                </asc:child>
                    <asc:ref-asc>ORGANIsation-ASD-044</asc:ref-asc>
                    <asc:description>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                            <asc:text>Basic Automatic Code Review</asc:text>
                        </asc:localized-information>
                    </asc:description>
                </asc:child>
                <asc:child>
                    <asc:ref-asc>ORGANIsation-ASD-045</asc:ref-asc>
                    <asc:description>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Advanced Automatic Code Review</asc:text>
                    </asc:description>
                </asc:child>
                <asc:child>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Manual Code Review</asc:text>
                        </asc:localized-information>
                    </asc:description>
                </asc:child>
            </asc:children>
            <asc:objective>
                <!-- Content removed for simplification -->
            </asc:objective>
            <asc:security-activity>
                <!-- Content removed for simplification -->
            </asc:security-activity>
            <asc:verification-measurement>
                <!-- Content removed for simplification -->
            </asc:verification-measurement>
        </asc:content>
    <asc:approval-e-signatures>
        <!-- Content removed for simplification -->
```

Окончание таблицы А.3

```
        </asc:approval-e-signatures>
    </asc:asc>
</asc:package-content>
<asc:package-editor-e-signature>
    <!-- Content removed for simplification -->
    </asc:package-editor-e-signature>
</asc:asc-package>
```

Таблица А.4 — XML-пример МОБП ORGANIsation-ASD-042: анализ исходного кода, идентификация

```
<?xml version="1.0" encoding="UTF-8"?>
<asc:asc-package xmlns:asc="http://iso.org/ISO27034/ASC-structure" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xml-asc-package-schema-version="1.0.0.0">
<asc:package-content>
    <asc:package-identification>
        <!-- Content removed for simplification -->
    </asc:package-identification>
    <asc:asc xml-asc-schema-version="1.0.0.0">
        <asc:content>
            <asc:identification>
            <asc:uid>ORGANIsation-ASD-042</asc:uid>
            <asc:name>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Code Review</asc:text>
                </asc:localized-information>
                </asc:name>
            <asc:version number="1.3.6.0" date="2013-03-06" life-cycle-stage="ACTIVE">
                <asc:revision-note>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Categorization ASC was added in this version to ensure a homogenous application's
                        class classification.</asc:text>
                    </asc:localized-information>
                </asc:revision-note>
            </asc:version>
            <asc:date>2016-01-04</asc:date>
                <asc:description>
                    <asc:text>This ASC is used to help developers to perform a code review control for JAVA applications.</asc:text>
                    </asc:localized-information>
                </asc:description>
            <asc:author>
                <asc:name>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>Jules Verne</asc:text>
                    </asc:localized-information>
                </asc:name>
                <asc:coordinate location-name="Office">
                    <asc:organization>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                            <asc:text>ORGANIsation inc.</asc:text>
                        </asc:localized-information>
                    </asc:organization>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                            <asc:text>Application Security Department</asc:text>
                        </asc:localized-information>
```

Продолжение таблицы А.4

```
                </asc:department>
                <asc:emails>
                    <asc:email type="Office">JVernes@ORGANIsation.com</asc:email>
                </asc:emails>
                <asc:phones>
                    <asc:phone type="Office">+1.234.567.8901</asc:phone>
                </asc:phones>
                <asc:street-address>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>1234 Street ave W</asc:text>
                    </asc:localized-information>
                </asc:street-address>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>Beautiful city</asc:text>
                </asc:localized-information>
                </asc:city>
                <asc:provice-state>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>Quebec</asc:text>
                    </asc:localized-information>
                </asc:provice-state>
                <asc:country>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Canada</asc:text>
                    </asc:localized-information>
                </asc:country>
                </asc:coordinate>
            </asc:author>
        <asc:name>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Douglas Adams</asc:text>
            </asc:localized-information>
        </asc:name>
        <asc:coordinate location-name="Office">
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
            </asc:localized-information>
        </asc:organization>
        <asc:department>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
            </asc:localized-information>
        </asc:department>
        <asc:emails>
            <asc:email type="Office">DAdams@ORGANIsation.com</asc:email>
        </asc:emails>
        <asc:phones>
            <asc:phone type="Office">+1.109.876.5432</asc:phone>
        </asc:phones>
        <asc:street-address>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
            <asc:text>1234 Street ave W</asc:text>
        </asc:street-address>
        <asc:city>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Beautiful city</asc:text>
```

Продолжение таблицы А.4

```
            </asc:localized-information>
        </asc:city>
        <asc:provice-state>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Quebec</asc:text>
            </asc:localized-information>
        </asc:provice-state>
        <asc:country>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Canada</asc:text>
                    </asc:localized-information>
                </asc:country>
            </asc:coordinate>
        </asc:owner>
        <asc:children>
            <asc:child>
            <asc:ref-asc>ORGANIsation-ASD-043</asc:ref-asc>
                <asc:description>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Code Classification</asc:text>
                    </asc:localized-information>
                </asc:description>
            </asc:child>
        <asc:child>
        <asc:ref-asc>ORGANIsation-ASD-044</asc:ref-asc>
            <asc:description>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>Basic Automatic Code Review</asc:text>
                </asc:localized-information>
            </asc:description>
        </asc:child>
        <asc:child>
            <asc:ref-asc>ORGANIsation-ASD-045</asc:ref-asc>
                <asc:description>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Advanced Automatic Code Review</asc:text>
                    </asc:localized-information>
                </asc:description>
            </asc:child>
        <asc:child>
            <asc:ref-asc>ORGANIsation-ASD-046</asc:ref-asc>
            <asc:description>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>Manual Code Review</asc:text>
                </asc:localized-information>
            </asc:description>
        </asc:child>
        </asc:children>
    </asc:identification>
    <asc:objective>
        <!-- Content removed for simplification -->
    </asc:objective>
    <asc:security-activity>
```

Окончание таблицы А.4

```
                <!-- Content removed for simplification -->
            </asc:security-activity>
            <asc:verification-measurement>
                <!-- Content removed for simplification -->
            </asc:verification-measurement>
        </asc:content>
        <asc:approval-e-signatures>
            <!-- Content removed for simplification -->
        </asc:approval-e-signatures>
    </asc:asc>
</asc:package-content>
    <asc:package-editor-e-signature>
        <!-- Content removed for simplification -->
    </asc:package-editor-e-signature>
</asc:asc-package>
```

Таблица А.5 — XML-пример МОБП ORGANIsation-ASD-042: анализ исходного кода, назначение

```
<?xml version="1.0" encoding="UTF-8"?>
<asc:asc-package xmlns:asc="http://iso.org/ISO27034/ASC-structure" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xml-asc-package-schema-version="1.0.0.0">
    <asc:package-content>
        <asc:package-identification>
            <!-- Content removed for simplification -->
        </asc:package-identification>
        <asc:asc xml-asc-schema-version="1.0.0.0">
        <asc:content>
            <asc:identification>
                <asc:uid>ORGANIsation-ASD-042</asc:uid>
                <!-- Content removed for simplification -->
            </asc:identification>
            <asc:objective>
                <asc:objective-description>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Top-level ASC whose objective is to group the various leaf ASCs related to code review
                        in Java.</asc:text>
                    </asc:localized-information>
                </asc:objective-description>
                <asc:requirements-addressed>
                    <asc:requirement>
                        <!-- Content removed for simplification -->
                    </asc:requirement>
                </asc:requirements-addressed>
                <asc:assigned-levels-of-trust>
                    <asc:level-of-trust-ref>45F736847</asc:level-of-trust-ref>
                    <asc:level-of-trust-ref>76878654</asc:level-of-trust-ref>
                    <asc:level-of-trust-ref>9876D54</asc:level-of-trust-ref>
                    <asc:level-of-trust-ref>4576825</asc:level-of-trust-ref>
                    <asc:level-of-trust-ref>989A67547</asc:level-of-trust-ref>
                    <asc:level-of-trust-ref>932564543</asc:level-of-trust-ref>
                </asc:assigned-levels-of-trust>
                <asc:contexts-of-use>
                    <asc:context type="Regulatory">TECHNOLOGICAL</asc:context>
                </asc:contexts-of-use>
                <asc:levels-of-trust-range>
```

Продолжение таблицы А.5

```
<asc:level-of-trust>
    <asc:level-of-trust-ref>45F736847</asc:level-of-trust-ref>
    <asc:level>0</asc:level>
    <asc:label>
        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
            <asc:text>Baseline</asc:text>
        </asc:localized-information>
    </asc:label>
    <asc:description>
        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
        <asc:text>All ORGANIsation's applications shall comply with this Level of Trust.</asc:text>
        </asc:localized-information>
    </asc:level-of-trust>
<asc:level-of-trust>
    <asc:level-of-trust-ref>76878654</asc:level-of-trust-ref>
    <asc:level>1</asc:level>
    <asc:label>
        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
        <asc:text>Isolated – Local network only</asc:text>
        </asc:localized-information>
    </asc:label>
    <asc:description>
        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
            <asc:text>This Level of Trust is appropriate for applications used on isolated corporate networks, with no connection to external networks.</asc:text>
        </asc:localized-information>
    </asc:description>
</asc:level-of-trust>
<asc:level-of-trust>
    <asc:level-of-trust-ref>9876D54</asc:level-of-trust-ref>
    <asc:level>2</asc:level>
    <asc:label>
        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
        <asc:text>Low – Internet, public information only</asc:text>
        </asc:localized-information>
    </asc:label>
    <asc:description>
        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
            <asc:text>This Level of Trust is appropriate for Internet-facing applications sharing public information without any privacy concern.</asc:text>
        </asc:localized-information>
    </asc:description>
</asc:level-of-trust>
<asc:level-of-trust>
    <asc:level-of-trust-ref>4576825</asc:level-of-trust-ref>
    <asc:level>3</asc:level>
    <asc:label>
        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
        <asc:text>Medium – Internet, corporate users</asc:text>
        </asc:localized-information>
    </asc:label>
    <asc:description>
        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
```

Продолжение таблицы А.5

```
                    <asc:text>This Level of Trust is appropriate for Internet-facing, transactional applications used
                    by corporate users, allowing access to corporate services, user files and/or transactions under
                    5,000 $.</asc:text>
                </asc:localized-information>
            </asc:description>
        </asc:level-of-trust>
        <asc:level-of-trust>
            <asc:level-of-trust-ref>989A67547</asc:level-of-trust-ref>
            <asc:level>4</asc:level>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>High – Secure transactions and privacy protection over Internet</asc:text>
                </asc:localized-information>
            </asc:label>
            <asc:description>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>This Level of Trust is appropriate for Internet-facing, transactional applications,
                        used by corporate users, allowing access to user private information and/ or transactions
                        from $5 000 to $25 000</asc:text>
                    </asc:localized-information>
                </asc:description>
            </asc:level-of-trust>
            <asc:level-of-trust>
                <asc:level-of-trust-ref>932564543</asc:level-of-trust-ref>
                <asc:level>5</asc:level>
                <asc:label>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Private</asc:text>
                    </asc:localized-information>
                </asc:label>
                <asc:description>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>This Level of Trust is appropriate for transactional applications requiring highly
                        secure transactions, privileged access and/or secure critical storage. Access to critical
                        information and/or transactions over $25 000 is authorized.</asc:text>
                    </asc:localized-information>
                </asc:description>
            </asc:level-of-trust>
        </asc:levels-of-trust-range>
        <asc:pre-conditions>
            <asc:condition>
                <!-- Content removed for simplification -->
            </asc:condition>
        </asc:pre-conditions>
    </asc:objective>
    <asc:security-activity>
        <!-- Content removed for simplification -->
    </asc:security-activity>
    <asc:verification-measurement>
        <!-- Content removed for simplification -->
    </asc:verification-measurement>
</asc:content>
<asc:approval-e-signatures>
    <!-- Content removed for simplification -->
</asc:approval-e-signatures>
```

Окончание таблицы А.5

```
    </asc:asc>
</asc:package-content>
    <asc:package-editor-e-signature>
        <!-- Content removed for simplification -->
    </asc:package-editor-e-signature>
</asc:asc-package>
```

Таблица А.6 — XML-пример МОБП ORGANIsation-ASD-043: классификация кода, назначение

```
<?xml version="1.0" encoding="UTF-8"?>
<asc:asc-package xmlns:asc="http://iso.org/ISO27034/ASC-structure" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xml-asc-package-schema-version="1.0.0.0">
    <asc:package-content>
    <asc:package-identification>
        <!-- Content removed for simplification -->
    </asc:package-identification>
    <asc:asc xml-asc-schema-version="1.0.0.0">
        <asc:content>
        <asc:identification>
            <asc:uid>ORGANIsation-ASD-043</asc:uid>
            <!-- Content removed for simplification -->
        </asc:identification>
        <asc:objective>
            <asc:objective-description>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>Define the scope of the code review.</asc:text>
                </asc:localized-information>
            </asc:objective-description>
        <asc:requirements-addressed>
            <asc:requirement>
            <asc:requirement-type>BUSINESS_REQUIREMENTS</asc:requirement-type>
            <asc:name>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Code Components Categorization Guidance</asc:text>
                    <asc:supporting-documents>
                        <asc:document>
                            <asc:name>ORGANIsation Development guidelines v2.1</asc:name>
                            <asc:description>ORGANIsation Development guidelines v2.1, Section 5.6 – Application
                            components classification.</asc:description>
                            <asc:binary-data>UjBsR09EbGhjZ0dTQUxNQUNBRU1t ... Q1p0dU1GUXhEUzhi</asc:binary-data>
                        </asc:document>
                    </asc:supporting-documents>
                </asc:localized-information>
            </asc:name>
            </asc:requirement>
        </asc:requirements-addressed>
        <asc:assigned-levels-of-trust>
            <asc:level-of-trust-ref>45F736847</asc:level-of-trust-ref>
            <asc:level-of-trust-ref>76878654</asc:level-of-trust-ref>
            <asc:level-of-trust-ref>9876D54</asc:level-of-trust-ref>
            <asc:level-of-trust-ref>4576825</asc:level-of-trust-ref>
            <asc:level-of-trust-ref>989A67547</asc:level-of-trust-ref>
            <asc:level-of-trust-ref>932564543</asc:level-of-trust-ref>
        </asc:assigned-levels-of-trust>
        <asc:levels-of-trust-range>
```

Продолжение таблицы А.6

```
        <asc:level-of-trust>
            <asc:level-of-trust-ref>45F736847</asc:level-of-trust-ref>
            <asc:level>0</asc:level>
            <asc:label>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>Baseline</asc:text>
                </asc:localized-information>
            </asc:label>
            <asc:description>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>All ORGANIsation's applications shall comply with this Level of Trust.</asc:text>
                </asc:localized-information>
            </asc:description>
        </asc:level-of-trust>
    <asc:level-of-trust>
        <asc:level-of-trust-ref>76878654</asc:level-of-trust-ref>
        <asc:level>1</asc:level>
        <asc:label>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
            <asc:text>Isolated – Local network only</asc:text>
            </asc:localized-information>
        </asc:label>
        <asc:description>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>This Level of Trust is appropriate for applications used on isolated corporate networks, with
                no connection to external networks.</asc:text>
            </asc:localized-information>
        </asc:description>
    </asc:level-of-trust>
    <asc:level-of-trust>
        <asc:level-of-trust-ref>9876D54</asc:level-of-trust-ref>
        <asc:level>2</asc:level>
        <asc:label>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
            <asc:text>Low – Internet, public information only</asc:text>
            </asc:localized-information>
        </asc:label>
        <asc:description>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>This Level of Trust is appropriate for Internet-facing applications sharing public information
                without any privacy concern.</asc:text>
            </asc:localized-information>
        </asc:description>
    </asc:level-of-trust>
    <asc:level-of-trust>
        <asc:level-of-trust-ref>4576825</asc:level-of-trust-ref>
        <asc:level>3</asc:level>
        <asc:label>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
            <asc:text>Medium – Internet, corporate users</asc:text>
            </asc:localized-information>
        </asc:label>
        <asc:description>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
```

Продолжение таблицы А.6

```
                    <asc:text>This Level of Trust is appropriate for Internet-facing, transactional applications used by corporate users, allowing access to corporate services, user files and/or transactions under 5,000 $.</asc:text>
                </asc:localized-information>
            </asc:description>
        </asc:level-of-trust>
        <asc:level-of-trust>
            <asc:level-of-trust-ref>989A67547</asc:level-of-trust-ref>
            <asc:level>4</asc:level>
            <asc:label>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>High – Secure transactions and privacy protection over Internet</asc:text>
                </asc:localized-information>
            </asc:label>
            <asc:description>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>This Level of Trust is appropriate for Internet-facing, transactional applications, used by corporate users, allowing access to user private information and/ or transactions from 5,000$ to 25,000$</asc:text>
                </asc:localized-information>
            </asc:description>
        </asc:level-of-trust>
        <asc:level-of-trust>
            <asc:level-of-trust-ref>932564543</asc:level-of-trust-ref>
            <asc:level>5</asc:level>
            <asc:label>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>Private</asc:text>
                </asc:localized-information>
            </asc:label>
            <asc:description>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>This Level of Trust is appropriate for transactional applications requiring highly secure transactions, privileged access and/or secure critical storage. Access to critical information and/or transactions over 25,000$ is authorized.</asc:text>
                </asc:localized-information>
            </asc:description>
        </asc:level-of-trust>
    </asc:levels-of-trust-range>
    <asc:pre-conditions>
        <asc:condition>
            <!-- Content removed for simplification -->
        </asc:condition>
    </asc:pre-conditions>
</asc:objective>
<asc:security-activity>
    <!-- Content removed for simplification -->
</asc:security-activity>
<asc:verification-measurement>
<!-- Content removed for simplification -->
</asc:verification-measurement>
</asc:content>
<asc:approval-e-signatures>
    <!-- Content removed for simplification -->
```

Окончание таблицы А.6

```
                    </asc:approval-e-signatures>
                </asc:asc>
            </asc:approval-e-signatures>
        </asc:asc>
    </asc:package-content>
    <asc:package-editor-e-signature>
        <!-- Content removed for simplification -->
    </asc:package-editor-e-signature>
</asc:asc-package>
```

Таблица А.7 — XML-пример МОБП ORGANIsation-ASD-043: классификация кода, мероприятия по обеспечению безопасности

```
<?xml version="1.0" encoding="UTF-8"?>
<asc:asc-package xmlns:asc="http://iso.org/ISO27034/ASC-structure" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xml-asc-package-schema-version="1.0.0.0">
    <asc:package-content>
    <asc:package-identification>
        <!-- Content removed for simplification -->
    </asc:package-identification>
    <asc:asc xml-asc-schema-version="1.0.0.0">
    <asc:content>
        <asc:identification>
            <asc:uid>ORGANIsation-ASD-043</asc:uid>
            <!-- Content removed for simplification -->
        </asc:identification>
        <asc:objective>
            <!-- Content removed for simplification -->
        </asc:objective>
        <asc:security-activity>
            <asc:activity-synopsis>
                <asc:name>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Classify classes and packages</asc:text>
                    </asc:localized-information>
                </asc:name>
                <asc:general-description>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Identify and categorize the application's Java classes and packages.</ asc:text>
                    </asc:localized-information>
                </asc:general-description>
                <asc:target-information>
                    <asc:infomation-item>
                        <asc:information-group>APPLICATION_DATA</asc:information-group>
                            <asc:nformation-sub-group>
                                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                                    <asc:text>Development documentation</asc:text>
                                </asc:localized-information>
                            </asc:nformation-sub-group>
                        <asc:name>
                            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                                <asc:text>Application's Java code architecture</asc:text>
                            </asc:localized-information>
                        </asc:name>
                    </asc:infomation-item>
```

Продолжение таблицы А.7

```
            </asc:target-information>
            <asc:outcome-general-description>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>Categorized classes and packages information merged in the application's Java code
                    architecture documentation.</asc:text>
                </asc:localized-information>
            </asc:outcome-general-description>
            <asc:supporting-expert-ressource>
                <asc:name>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Orson Scott Card</asc:text>
                    </asc:localized-information>
                </asc:name>
                <asc:coordinate location-name="String">
                    <asc:organization>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                            <asc:text>ORGANIsation inc.</asc:text>
                        </asc:localized-information>
                    </asc:organization>
                    <asc:emails>
                        <asc:email type="Office">Orson.Scott.Card@ORGANIsation.com</asc:email>
                    </asc:emails>
                </asc:coordinate>
            </asc:supporting-expert-ressource>
        </asc:activity-synopsis>
        <asc:activity-complexity>
            <asc:label>COMPLEX</asc:label>
            <asc:complexity-description>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text> This activity should be performed by someone able to identify, from the application ar-
                    chitecture documents, what information is manipulated by each Java class and to identify security
                    risks that may threaten sensitive information.</asc:text>
                </asc:localized-information>
            </asc:complexity-description>
            <asc:global-estimated-description>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>- Average of 1 hour to classify and document 10 Java classes.
                    - Average of 15 hours to update the Application Security Risk Analysis.</asc:text>
                </asc:localized-information>
            </asc:global-estimated-description>
            <asc:global-estimated-effort unit="HOURS">35</asc:global-estimated-effort>
        </asc:activity-complexity>
        <asc:activity-specification>
            <asc:task seq="0">
            <asc:task-description>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>Classify all classes and packages of the application.</asc:text>
                </asc:localized-information>
            </asc:task-description>
            <asc:required-resources>
                <asc:resource-allocation>
                    <asc:role>APPLICATION_ARCHITECT</asc:role>
                    <asc:responsibility>RESPONSIBLE</asc:responsibility>
                        <asc:task-description>
```

Продолжение таблицы А.7

```
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Classify the application classes to be developed or maintained in this project.</asc:text>
                    </asc:localized-information>
                </asc:task-description>
                <asc:task-complexity>
                <asc:label>COMPLEX</asc:label>
                <asc:complexity-description>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>This activity should be done by someone who is able to identify, from applicaton
                        acthitecture documents, what information is manipulated in every Java classes and identify
                        security risks that may threat sensible information.</asc:text>
                    </asc:localized-information>
                </asc:complexity-description>
                <asc:global-estimated-description>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>- Average of 60 minutes to classify and document 10 Java classes.
                        - Average of 15 hours to update the Application Security Risk Analysis.</asc:text>
                    </asc:localized-information>
                </asc:global-estimated-description>
            </asc:task-complexity>
                <asc:required-qualifications>
                <asc:qualification status="MUST_HAVE">
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Passed an examination on the ORGANIsation Java coding best practices.</asc:text>
                    </asc:localized-information>
                </asc:qualification>
                <asc:qualification status="MUST_HAVE">
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Minimum 5 years experience in Java Development.</asc:text>
                    </asc:localized-information>
                </asc:qualification>
                <asc:qualification status="MUST_HAVE">
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>Active CSSLP Certification.</asc:text>
                    </asc:localized-information>
                </asc:qualification>
            </asc:required-qualifications>
        </asc:resource-allocation>
    </asc:required-resources>
    <asc:pre-conditions>
        <asc:condition>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>The application classes and packages identification section of the Application design
                document is completed.</asc:text>
            </asc:localized-information>
        </asc:condition>
        <asc:condition>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>A list of categorized information groups involved by the application already exists.</asc:text>
            </asc:localized-information>
        </asc:condition>
    </asc:pre-conditions>
    <asc:localization>
        <asc:location>
```

Продолжение таблицы А.7

```
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Application development environment</asc:text>
            </asc:localized-information>
        </asc:location>
    </asc:localization>
    <asc:action-list>
        <asc:action seq="0">
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Identify contexts, roles, and information involved with the application module.</asc:text>
                <asc:supporting-documents>
                    <asc:document>
                        <asc:name>ORGANIsation Development guidelines v2.1</asc:name>
                        <asc:description>ORGANIsation Development guidelines v2.1.PDF</asc:description>
                        <asc:binary-data>UjBsR09EbGhjZ0dTQUxNQU ... FBUUNBRU1tQ1</asc:binary-data>
                    </asc:document>
                </asc:supporting-documents>
            </asc:localized-information>
        </asc:action>
        <asc:action seq="1">
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Realize or update the Application Security Risk Analysis.</asc:text>
            </asc:localized-information>
        </asc:action>
        <asc:action seq="2">
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Classify all classes in the packages needed by the application in the Application Class
                Classification section of the Application design document.</asc:text>
                <asc:supporting-documents>
                    <asc:document>
                        <asc:name>ORGANIsation Code Classification Guide, v1.4</asc:name>
                        <asc:description>ORGANIsation Code Classification Guide, v1.4.PDF</asc:description>
                        <asc:binary-data>UjBsR09EbGhjZ0dT ... 1tQ1p0dU1GUXhEUzhi</asc:binary-data>
                    </asc:document>
                    <asc:document>
                        <asc:name>Application Class Classification section – Template v2.3</asc:name>
                        <asc:description>Application Class Classification section – Template v2.3.RTF</asc:description>
                        <asc:binary-data>UjBUXhEUzhisR0dT ... 1tQ1p09EbGhjZ0dU1G</asc:binary-data>
                    </asc:document>
                </asc:supporting-documents>
            </asc:localized-information>
        </asc:action>
    </asc:action-list>
    <asc:execution-moments>
        <asc:moment>
            <asc:order>AFTER</asc:order>
            <asc:description>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>The detailed application architecture is completed.</asc:text>
                </asc:localized-information>
            </asc:description>
            <asc:life-cycle-reference>
                <!-- Content removed for simplification -->
            </asc:life-cycle-reference>
                <asc:interval-value frequence="ONCE" unit="PROJECT">0</asc:interval-value>
```

Окончание таблицы А.7

```
                    </asc:moment>
                </asc:execution-moments>
                <asc:outcome>
                    <asc:produced-artefact>
                        <asc:type>DOCUMENT</asc:type>
                        <asc:content>
                            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                                <asc:text> The Application Module Classification section, in the Application design document, describing for all application modules, their class classification value from “Not critical” to “Critical”.</asc:text>
                            </asc:localized-information>
                        </asc:content>
                    </asc:produced-artefact>
                    <asc:produced-artefact>
                        <asc:type>DOCUMENT</asc:type>
                        <asc:content>
                            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                                <asc:text>The classification method, templates and examples are described in the classification Guide, referenced within this ASC.</asc:text>
                            </asc:localized-information>
                        </asc:content>
                    </asc:produced-artefact>
                </asc:outcome>
            </asc:task>
        </asc:activity-specification>
    </asc:security-activity>
    <asc:verification-measurement>
        <!-- Content removed for simplification -->
    </asc:verification-measurement>
</asc:content>
<asc:approval-e-signatures>
    <!-- Content removed for simplification -->
</asc:approval-e-signatures>
</asc:asc>
</asc:package-content>
<asc:package-editor-e-signature>
<!-- Content removed for simplification -->
</asc:package-editor-e-signature>
</asc:asc-package>
```

Таблица А.8 — XML-пример МОБП ORGANIsation-ASD-043: классификация кода, проверочные измерения

```
<?xml version="1.0" encoding="UTF-8"?>
<asc:asc-package xmlns:asc="http://iso.org/ISO27034/ASC-structure" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xml-asc-package-schema-version="1.0.0.0">
<asc:package-content>
<asc:package-identification>
    <!-- Content removed for simplification -->
</asc:package-identification>
<asc:asc xml-asc-schema-version="1.0.0.0">
<asc:content>
    <asc:identification>
        <asc:uid>ORGANIsation-ASD-043</asc:uid>
            <!-- Content removed for simplification -->
    </asc:identification>
```

Продолжение таблицы А.8

```
<asc:objective>
    <!-- Content removed for simplification -->
</asc:objective>
<asc:security-activity>
    <!-- Content removed for simplification -->
</asc:security-activity>
<asc:verification-measurement>
    <asc:activity-synopsis>
        <asc:name>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Classes and packages classification verification.</asc:text>
            </asc:localized-information>
        </asc:name>
        <asc:general-description>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Verify if the application's Java classes and packages produced or modified were
                adequatly categorized.</asc:text>
            </asc:localized-information>
        </asc:general-description>
        <asc:target-information>
            <asc:infomation-item>
                <asc:information-group>APPLICATION_DATA</asc:information-group>
                    <asc:nformation-sub-group>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                            <asc:text>Application development documentation</asc:text>
                        </asc:localized-information>
                    </asc:nformation-sub-group>
                <asc:name>
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Application's Java code architecture</asc:text>
                    </asc:localized-information>
                </asc:name>
            </asc:infomation-item>
        </asc:target-information>
        <asc:outcome-general-description>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>These two documents are produced or updated: the Application security risk analysis
                and the Application design document.</asc:text>
            </asc:localized-information>
        </asc:outcome-general-description>
        <asc:supporting-expert-ressource>
            <asc:name>
                <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                    <asc:text>Ray Bradbury</asc:text>
                </asc:localized-information>
            </asc:name>
            <asc:coordinate location-name="Office">
                <asc:emails>
                    <asc:email type="Office">Ray.Bradbury@ORGANIsation.com</asc:email>
                </asc:emails>
            </asc:coordinate>
        </asc:supporting-expert-ressource>
    </asc:activity-synopsis>
    <asc:activity-complexity>
```

Продолжение таблицы А.8

```
<asc:label>COMPLEX</asc:label>
<asc:complexity-description>
  <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
    <asc:text> This activity should be done by someone who is able to validate, from applicaton
    architecture documents, what information is manipulated in every Java classes and to validate
    security risks that may threaten sensitive information.</asc:text>
  </asc:localized-information>
</asc:complexity-description>
<asc:global-estimated-description>
  <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
    <asc:text>An average of 6 hours to validate the contexts and revise the risk analysis and an
    average of 10 minutes to approve/reject each class and package.</asc:text>
  </asc:localized-information>
</asc:global-estimated-description>
<asc:global-estimated-effort unit="HOURS">12</asc:global-estimated-effort>
</asc:activity-complexity>
<asc:activity-specification>
<asc:task seq="0">
  <asc:task-description>
    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
      <asc:text>Classify application's classes and components</asc:text>
        <asc:supporting-documents>
          <asc:document>
            <asc:name>ORGANIsation Code Classification Guide, v1.4</asc:name>
            <asc:description>ORGANIsation Code Classification Guide, v1.4.PDF</asc:description>
            <asc:binary-data>UjBsR9EbGhjZ0 ... dTQUxFBUUNBRU1tQ1p0dU1GUXhEUzhi
            </asc:binary-data>
          </asc:document>
        </asc:supporting-documents>
    </asc:localized-information>
  </asc:task-description>
<asc:required-resources>
  <asc:resource-allocation>
    <asc:role>APPLICATION_SECURITY_ARCHITECT</asc:role>
    <asc:responsibility>ACCOUNTABLE</asc:responsibility>
    <asc:responsibility>RESPONSIBLE</asc:responsibility>
    <asc:task-description>
      <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
        <asc:text> Revise and approve Application Module Classification section, in the Application
        design document.</asc:text>
        <asc:supporting-documents>
          <asc:document>
            <asc:name>ORGANIsation Code Classification Guide, v1.4</asc:name>
              <asc:description>ORGANIsation Code Classification Guide, v1.4.PDF</asc:description>
            <asc:binary-data>GhjZ0dTQUxNQU ... FBUUN1GUXhEUzhi</asc:binary-data>
          </asc:document>
        </asc:supporting-documents>
      </asc:localized-information>
    </asc:task-description>
    <asc:required-qualifications>
      <asc:qualification status="MUST_HAVE">
        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
          <asc:text>Passed an examination on the ORGANIsation Java coding best practices.</asc:text>
        </asc:localized-information>
```

Продолжение таблицы А.8

```
                </asc:qualification>
                <asc:qualification status="MUST_HAVE">
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Passed an examination on the secure application architecture.</asc:text>
                    </asc:localized-information>
                </asc:qualification>
                <asc:qualification status="MUST_HAVE">
                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                        <asc:text>Active CSSLP Certification.</asc:text>
                    </asc:localized-information>
                </asc:qualification>
            </asc:required-qualifications>
        </asc:resource-allocation>
    </asc:required-resources>
    <asc:pre-conditions>
        <asc:condition>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>The Application's Java code architecture documentation includes a complete
                categorized classes and packages information.</asc:text>
            </asc:localized-information>
        </asc:condition>
    </asc:pre-conditions>
    <asc:localization>
        <asc:location>
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Application development environment</asc:text>
            </asc:localized-information>
        </asc:location>
    </asc:localization>
    <asc:action-list>
        <asc:action seq="0">
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Validate the contexts, roles and information involved with this module.</asc:text>
            </asc:localized-information>
        </asc:action>
        <asc:action seq="1">
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>Revise the application risk analysis.</asc:text>
            </asc:localized-information>
        </asc:action>
        <asc:action seq="2">
            <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                <asc:text>For each class, reject or approve the classification and mark accordingly.</asc:text>
            </asc:localized-information>
        </asc:action>
    </asc:action-list>
    <asc:execution-moments>
        <asc:moment>
            <asc:order>BEFORE</asc:order>
                    <asc:description>
                        <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                            <asc:text>Coding.</asc:text>
                        </asc:localized-information>
```

Окончание таблицы А.8

```
                                </asc:description>
                                <asc:life-cycle-reference>
                                    <!-- Content removed for simplification -->
                                </asc:life-cycle-reference>
                                <asc:interval-value frequence="ONCE" unit="PROJECT">0</asc:interval-value>
                            </asc:moment>
                        </asc:execution-moments>
                        <asc:outcome>
                            <asc:produced-artefact>
                                <asc:type>DOCUMENTS</asc:type>
                                <asc:content>
                                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                                        <asc:text>Updated Application security risk analysis document.</asc:text>
                                    </asc:localized-information>
                                </asc:content>
                            </asc:produced-artefact>
                            <asc:produced-artefact>
                                <asc:type>DOCUMENTS</asc:type>
                                <asc:content>
                                    <asc:localized-information language="EN" country="CA" organization="ORGANIsation">
                                        <asc:text>Approved Application Module Classification section, in the Application
                                        design document.</asc:text>
                                    </asc:localized-information>
                                </asc:content>
                            </asc:produced-artefact>
                        </asc:outcome>
                    </asc:task>
                </asc:activity-specification>
            </asc:verification-measurement>
        </asc:content>
        <asc:approval-e-signatures>
            <!-- Content removed for simplification -->
        </asc:approval-e-signatures>
    </asc:asc>
</asc:package-content>
<asc:package-editor-e-signature>
    <!-- Content removed for simplification -->
</asc:package-editor-e-signature>
</asc:asc-package>
```

Библиография

[1] ISO 3166-1, Codes for the representation of names of countries and their subdivisions — Part 1: Country codes
[2] ISO/IEC 27034-1:2011, Information technology — Security techniques — Application security — Part 1: Overview and concepts
[3] ISO/IEC 27034-2, Information technology — Security techniques — Application security — Part 2: Organization normative framework
[4] ISO/IEC 27034-5, Information technology — Security techniques — Application security — Part 5: Protocols and application security control data structure
[5] ISO/IEC 27034-5-1, Information technology — Security techniques — Application security — Part 5-1: Protocols and application security controls data structure — XML schemas

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

Ключевые слова: безопасность приложений, нормативная структура организации (НСО), меры обеспечения безопасности приложений (МОБП), нормативная структура приложения (НСП), жизненный цикл безопасности приложений (ЖЦБП)

Технический редактор *В.Н. Прусакова*
Корректор *Л.С. Лысенко*
Компьютерная верстка *Е.О. Асташина*

Сдано в набор 19.05.2021. Подписано в печать 17.06.2021. Формат 60×84⅛. Гарнитура Ариал.
Усл. печ. л. 7,91. Уч.-изд. л. 7,15.

Подготовлено на основе электронной версии, предоставленной разработчиком стандарта

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