НАЦИОНАЛЬНЫЙ СТАНДАРТ КЫРГЫЗСКОЙ РЕСПУБЛИКИ

Маалымат технологиясы
КООПСУЗДУКТУ КАМСЫЗ КЫЛУУНУН ЫКМАЛАРЫ ЖАНА КАРАЖАТТАРЫ
Колдонмонун коопсуздугу
1-бөлүк
Карап чыгуу жана жалпы түшүнүктөр

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
Безопасность приложений
Часть 1
Обзор и общие понятия

(ГОСТ Р ИСО-МЭК 27034-1-2014, IDT)

Издание официальное

ЦСМ

Бишкек

Предисловие

Цели, принципы и основные положения стандартизации в Кыргызской Республике установлены законом Кыргызской Республики «О техническом регулировании в Кыргызской Республике» и КМС 1.0

Сведения о стандарте

1 ПОДГОТОВЛЕН Центром по стандартизации и метрологии при Министерстве экономики и коммерции Кыргызской Республики (Кыргызстандарт)

2 ВНЕСЕН Государственным агентством по земельным ресурсам, кадастру, геодезии и картографии при Кабинете Министров Кыргызской Республики

3 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Центра по стандартизации и метрологии при Министерстве экономики и коммерции Кыргызской Республики (Кыргызстандарт) от 15 августа 2024 г. № 35-СТ.

4 Настоящий стандарт идентичен ГОСТ Р ИСО-МЭК 27034-1-2014, Информационная технология. Методы и средства обеспечения безопасности. Безопасность приложений. Часть 1. Обзор и общие понятия

5 ВВЕДЕН впервые

Содержание

Введение

0.1 Общая информация

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

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

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

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

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

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

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

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

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

0.2 Назначение

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

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

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

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

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

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

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