**Пояснительная записка**

**к проекту национального стандарта**

**СТ РК ГОСТ Р 56939 «Защита информации. Безопасная разработка программного обеспечения. Общие требования»**

**1 Техническое обоснование разработки проекта документа по стандартизации**

В пункте 45 Единых требований в области информационно-коммуникационных технологий и обеспечения информационной безопасности (утверждены постановлением Правительства Республики Казахстан от 20 декабря 2016 года № 832) (далее – Единые требования) имеется ссылка на необходимость исполнения требований СТ РК 15408 «Информационные технологии. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий».

В 2024 году РГП на ПХВ «Казахстанский институт стандартизации и метрологии» (далее - Казстандарт) разработан СТ РК ISO/IEC 15408-3-2024 «Информационная безопасность, кибербезопасность и защита конфиденциальности. Критерии оценки безопасности информационных технологий. Часть 3. Компоненты обеспечения безопасности» (далее – СТ РК 15408-3) взамен действующего СТ РК ISO/IEC 15408-3-2017.

В тоже время, в СТ РК 15408-3 указывается о необходимости безопасной разработки программного обеспечения. Так, в пункте 5.3.3. «Причина уязвимости» указано, что уязвимости могут возникать из-за недостатков в разработке, т.е продукт не соответствует своим спецификациям и/или в результате плохих стандартов разработки или неправильного выбора дизайна появились уязвимости. Также, в пункте 10 «Класс ADV: Разработка» проекта СТ РК 15408-3 указывается о необходимости безопасной разработки. Кроме того в пункте 12.5.4 «ALC\_DVS.1 Идентификация мер безопасности» указано, что разработчик должен представить документацию по безопасности разработки, которая должна содержать описание всех физических, процедурных, организационных и других мер безопасности, которые необходимы для защиты конфиденциальности и целостности проекта и его реализации в среде разработки.

Однако в Казахстане, отсутствует утвержденный национальный стандарт по безопасной разработки программного обеспечения, что препятствует эффективному соблюдению положений СТ РК 15408-3 по безопасной разработке.

В связи с этим, предлагается разработка национального стандарта, который будет направлен на достижение целей, связанных с предотвращением появления, выявлением и устранением уязвимостей и недекларированных возможностей в программном обеспечении, и будет содержать общие требования, предъявляемые к разработчикам программного обеспечения при реализации процессов разработки безопасного программного обеспечения.

После разработки стандарта СТ РК «Безопасная разработка программного обеспечения. Общие требования» (далее – СТ РК) будет проводится работа по включению в пункт 45 Единых требований ссылочных норм о соблюдении требований данного   
СТ РК.

2 Основание для разработки документа по стандартизации

Национальный план стандартизации на 2025 год, утвержденный приказом Председателя Комитета технического регулирования и метрологии Министерства торговли и интеграции Республики Казахстан от 31 декабря 2024 года № 447-НҚ (с учетом дополнений, внесенных приказом от «26» февраля 2025 года № 17-НҚ).

**3 Характеристика объекта стандартизации**

Объектом стандартизации является безопасная разработка программного обеспечения, аспект стандартизации – общие требования.

**4 Сведения о взаимосвязи проекта документа по стандартизации с техническими регламентами и документами по стандартизации**

Отсутствует.

**5 Предполагаемые пользователи проекта документа по стандартизации**

Предполагаемыми пользователями национального стандарта являются – Комитет по информационной безопасности Министерства цифрового развития, инноваций и аэрокосмической промышленности, АО «ГТС», АО «НИТ», МЦРИАП РК, КНБ РК, разработчики и производители программного обеспечения.

**6 Сведения о рассылке проекта документа по стандартизации на согласование**

Проект национального стандарта направлен на согласование и рассмотрение заинтересованным организациям и государственным органам.

**7 Информация о результатах научных исследований (испытаний) и измерений, документах по стандартизации и иных документах, на основе которых разрабатывается проект документа по стандартизации**

Настоящий проект стандарта разработан с учетом требований национального стандарта Российской Федерации ГОСТ Р 56939-2016 «Защита информации. Разработка безопасного программного обеспечения. Общие требования».

**8 Данные о разработчике и соисполнителях (контактные данные), сроках разработки документа по стандартизации**

РГП на ПХВ «Казахстанский институт стандартизации и метрологии»

г. Астана, пр. Мәнгілік Ел, д. 11, здание «Эталонный Центр»

Тел. +7 (7172) 75-59-38

Е-mail: info@ksm.kz, zh.tuyakov@ksm.kz

**Руководитель**

**Департамента разработки стандартов Сопбеков А.Н.**