

## **Пояснительная записка**

к проекту национального стандарта

ГОСТ Р «Защита информации. Формальное моделирование политики безопасности.

Часть 1. Формальная модель управления доступом»

(первая редакция)

(шифр темы ПНС — 1.11.362-1.001.19)

### **1. ОСНОВАНИЕ ДЛЯ РАЗРАБОТКИ НАЦИОНАЛЬНОГО СТАНДАРТА**

Настоящий проект национального стандарта ГОСТ Р «Защита информации. Формальное моделирование политики безопасности. Часть 1. Формальная модель управления доступом» разрабатывается в соответствии с Программой разработки национальных стандартов на 2019 год по техническому комитету по стандартизации «Защита информации» (ТК 362).

### **2. КРАТКАЯ ХАРАКТЕРИСТИКА ОБЪЕКТА СТАНДАРТИЗАЦИИ**

Объектом стандартизации разрабатываемого проекта национального стандарта являются требования, предъявляемые к структуре, содержанию, языку описания формальных моделей управления доступом.

Проект национального стандарта ГОСТ Р «Защита информации. Формальное моделирование политики безопасности. Часть 1. Формальная модель управления доступом» включает следующие разделы:

- введение;
- область применения;
- термины и определения;
- общие положения;
- моделирование состояний абстрактного автомата;
- моделирование переходов абстрактного автомата из состояний в состояния;
- доказательство выполнения в абстрактном автомате условий безопасности.

Настоящий стандарт устанавливает общие требования к структуре и содержанию формальных моделей управления доступом, разрабатываемых в целях повышения доверия к принципам и общим подходам к управлению доступом, на основе которых формируются реализуемые в средствах защиты от несанкционированного доступа политики управления доступом (дискреционного, ролевого, мандатного управления

доступом, мандатного контроля целостности или другие виды политик управления доступом).

Настоящий стандарт предназначен для разработчиков средств защиты от несанкционированного доступа, применяющих научно обоснованные подходы к разработке, реализации и обеспечению совместимости политик управления доступом. Настоящий стандарт предназначен также для органов по сертификации и испытательных лабораторий при проведении оценки соответствия и сертификации средств защиты от несанкционированного доступа, реализующих политики управления доступом.

### **3. ОБОСНОВАНИЕ ЦЕЛЕСООБРАЗНОСТИ РАЗРАБОТКИ НАЦИОНАЛЬНОГО СТАНДАРТА И ОЖИДАЕМЫЙ ЭФФЕКТ ОТ ЕГО ПРИМЕНЕНИЯ**

В средствах защиты от несанкционированного доступа, как правило, реализуются политики безопасности, в том числе политики управления доступом. Повышение доверия к средствам защиты от несанкционированного доступа, применение при формировании политик управления доступом научно обоснованных подходов и международного опыта предполагают использование формальных моделей управления доступом. Многообразие существующих формальных моделей управления доступом, ориентированных на описание различных видов политик управления доступом (дискреционной, ролевой, мандатной и других видов политик), используемых для этого часто несовместимых языков, приемов и технологий описания и верификации формальных моделей, создает предпосылки для реализации средствами защиты от несанкционированного доступа несогласованных, противоречивых, научно необоснованных политик управления доступом.

Согласно настоящему стандарту моделирование политик управления доступом основывается на применении абстрактного автомата, что, в свою очередь, базируется на всесторонней научной и практической апробации этого подхода в средствах защиты от несанкционированного доступа, а также на том, что абстрактный автомат может рассматриваться как непосредственный прототип средства защиты от несанкционированного доступа, как программного, аппаратного или программно-аппаратного средства. При этом язык описания формальной модели управления доступом должен быть математическим или формализованным (машиночитаемым) и допускать полную независимую от разработчика формальной модели проверку корректности ее описания и всех выполненных в модели доказательств.

Принятие проекта национального стандарта ГОСТ Р «Защита информации. Формальное моделирование политики безопасности. Часть 1. Формальная модель

управления доступом» позволит повысить доверие к средствам защиты от несанкционированного доступа при реализации ими политик безопасности управления доступом на основе формальных моделей управления доступом.

#### **4. СВЕДЕНИЯ О СООТВЕТСТВИИ ПРОЕКТА НАЦИОНАЛЬНОГО СТАНДАРТА ЗАКОНОДАТЕЛЬСТВУ РОССИЙСКОЙ ФЕДЕРАЦИИ, МЕЖДУНАРОДНЫМ, РЕГИОНАЛЬНЫМ И НАЦИОНАЛЬНЫМ СТАНДАРТАМ ДРУГИХ СТРАН**

Проект национального стандарта разработан в соответствии с ГОСТ Р 1.5-2012 «Стандартизация в Российской Федерации. Стандарты национальные. Правила построения, изложения, оформления и обозначения».

#### **5. СВЕДЕНИЯ О ПАТЕНТНОЙ ЧИСТОТЕ ПРОЕКТА СТАНДАРТА**

При разработке проекта национального стандарта ГОСТ Р «Защита информации. Формальное моделирование политики безопасности. Часть 1. Формальная модель управления доступом» патенты не использовались.

#### **6. СВЕДЕНИЯ О ВЗАИМОСВЯЗИ ПРОЕКТА СТАНДАРТА С ДРУГИМИ НОРМАТИВНЫМИ ДОКУМЕНТАМИ ПО СТАНДАРТИЗАЦИИ И ПРЕДЛОЖЕНИЯ ПО ИХ ПЕРЕСМОТРУ, ИЗМЕНЕНИЮ ИЛИ ОТМЕНЕ**

Требования настоящего национального стандарта не применяются совместно с требованиями национальных стандартов Российской Федерации и не противоречат им, а поэтому пересмотр, изменение или отмена действующих документов не требуется.

#### **7. СВЕДЕНИЯ О СОГЛАСОВАНИИ**

Первая редакция проекта национального стандарта ГОСТ Р «Защита информации. Формальное моделирование политики безопасности. Часть 1. Формальная модель управления доступом» разработана в рамках СЧ НИР «Идентификация-Р», подготовлена в результате апробации в ФАУ «ГНИИИ ПТЗИ ФСТЭК России» и организациях-лицензиатах согласно утвержденному ФСТЭК России перечню, полученных от них отзывов на первую редакцию проекта национального стандарта, а также замечаний и предложений, высказанных в ходе технического совещания исполнителей СЧ НИР «Идентификация-Р», ФАУ «ГНИИИ ПТЗИ ФСТЭК России» и организаций-лицензиатов ФСТЭК России, проведенного 25 февраля 2019 г.

Первая редакция проекта национального стандарта предназначена для направления на рассмотрение в технический комитет по стандартизации «Защита информации» (ТК 362).

## 8. ИСТОЧНИКИ ИНФОРМАЦИИ

Источники информации отсутствуют.

Руководитель темы,  
Заместитель директора Центра  
компьютерных технологий  
АО «НПО РусБИТех»



А.Л. Оружейников