ГОСТЕХКОМИССИЯ РОССИИ

РУКОВОДЯЩИЙ ДОКУМЕНТ

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Критерии оценки безопасности информационных технологий

Введен в действие Приказом
Гостехкомиссии России
от 19.06.02 г. № 187

2002

gost.e-ecolog.ru

Общие положения

Настоящий руководящий документ (РД) содержит систематизированный каталог требований к безопасности информационных технологий (ИТ), порядок и методические рекомендации по его использованию при задании требований, разработке, оценке и сертификации продуктов и систем информационных технологий по требованиям безопасности информации.

Руководящий документ разработан в развитие РД Гостехкомиссии России по защите информации от несанкционированного доступа и соответствует ГОСТ Р ИСО/МЭК 15408-2002 "Информационная технология. Методы обеспечения безопасности. Критерии оценки безопасности информационных технологий", далее по тексту РД – Общие критерии (ОК).

Разработка настоящего руководящего документа направлена на обеспечение практического использования ГОСТ Р ИСО/МЭК 15408-2002 в деятельности заказчиков, разработчиков и пользователей продуктов и систем ИТ при формировании ими требований, разработке, приобретении и применении продуктов и систем информационных технологий, предназначенных для обработки, хранения или передачи информации, подлежащей защите в соответствии с требованиями нормативных правовых документов или требованиями, устанавливаемыми собственником информации. Руководящий документ предназначен также для органов сертификации и испытательных лабораторий, аккредитованных в системе сертификации средств защиты информации по требованиям безопасности информации № РОСС RU.0001.01БИ00 (Гостехкомиссии России), для использования при проведении оценки и сертификации безопасности ИТ.

Основной целью руководящего документа является повышение доверия к безопасности продуктов и систем информационных технологий. Положения руководящего документа направлены на создание продуктов и систем информационных технологий с уровнем безопасности, адекватным имеющимся по отношению к ним угрозам и проводимой политике безопасности с учетом условий применения, что должно обеспечить оптимизацию продуктов и систем ИТ по критерию "эффективность-стоимость".

Под безопасностью информационной технологии понимается состояние ИТ, определяющее защищенность информации и ресурсов ИТ от действия объективных и субъективных, внешних и внутренних, случайных и преднамеренных угроз, а также способность ИТ выполнять предписанные функции без нанесения неприемлемого ущерба субъектам информационных отношений.

Доверие к безопасности ИТ обеспечивается, как реализацией в них необходимых функциональных возможностей, так и осуществлением комплекса мер по обеспечению безопасности при разработке продуктов и систем ИТ, проведением независимых оценок их безопасности и контролем ее уровня при эксплуатации.

Требования к безопасности конкретных продуктов и систем ИТ устанавливаются исходя из имеющихся и прогнозируемых угроз безопасности, проводимой политики безопасности, а также с учетом условий их применения. При формировании требований должны в максимальной степени использоваться компоненты требований, представленные в настоящем руководящем документе. Допускается также использование и других требований безопасности, при этом уровень детализации и способ выражения требований, представленных в настоящем руководящем документе, должны использоваться в качестве образца. Требования безопасности могут задаваться Заказчиком в техническом задании на разработку продуктов и систем ИТ или формироваться Разработчиком при создании им продуктов ИТ самостоятельно.

Требования безопасности, являющиеся общими для некоторого типа продуктов или систем ИТ, могут оформляться в виде представленной в настоящем руководящем документе структуры, именуемой "Профиль защиты". Профили защиты, прошедшие оценку в установленном порядке, регистрируются и помещаются в каталог оцененных профилей защиты.

Оценка и сертификация безопасности ИТ проводится на соответствие требованиям, представляемым Разработчиком продукта или системы ИТ в Задании по безопасности. Требования заданий по безопасности продуктов и систем ИТ, предназначенных для использования в областях применения, регулируемых государством, должны соответствовать требованиям установленных профилей защиты.

Руководящий документ состоит из трех частей.

Часть 1 РД определяет виды требований безопасности (функциональные и требования доверия), основные конструкции представления требований безопасности (профиль защиты, задание по безопасности) и содержит основные методические положения по оценке безопасности ИТ.

Часть 2 РД содержит универсальный систематизированный каталог функциональных требований безопасности и предусматривает возможность их детализации и расширения по определенным правилам.

Часть 3 РД содержит систематизированный каталог требований доверия к безопасности и оценочные уровни доверия, определяющие меры, которые должны быть приняты на всех этапах жизненного цикла продуктов или систем ИТ для обеспечения уверенности в том, что они удовлетворяют предъявленным к ним функциональным требованиям.

Требования безопасности, содержащиеся в настоящем руководящем документе, могут уточняться и дополняться по мере совершенствования правовой и нормативной базы, развития информационных технологий и совершенствования методов обеспечения безопасности. Внесение изменений в руководящий документ осуществляется в порядке, устанавливаемом Гостехкомиссией России.

gost.e-ecolog.ru