**Единые критерии безопасности информационных технологий**

«Единые критерии безопасности информационных технологий» (Common Griteria for Information Technology Security Evaluation) является результатом совместных усилий авторов «Европейских критериев безопасности информационных технологий», «Федеральных критериев безопасности информационных технологий» и «Канадских критериев безопасности компьютерных систем», направленных на объединение основных положений этих документов и создание единого международного стандарта безопасности информационных технологий. Работа над этим стандартом началась в 93 году. Версия 2.1 этого стандарта утверждена Международной организацией по стандартизации (ISO) в 1999 году в качестве международного стандарта информационной безопасности ISO| IEC 15408. **В РФ стандарт действует под номером ГОСТ Р ИСО/МЭК 15408.** Этот документ разработан на основе достижений многочисленных исследований в области безопасности ИТ 90-ых годов и на результатах анализа опыта применения в положенных в его основу стандартов. Единые критерии оперируют уже знакомым по федеральным критериям понятиям продукт информационных технологий или айти продукт. И используют предложенную в них концепцию профиля защиты.

Единые критерии разрабатывались в расчёте на то, чтобы удовлетворить запросы 3-ёх групп специалистов:

1. Производителей;
2. Потребителей;
3. Экспертов по квалификации уровня их безопасности.

**Потребители рассматривают квалификацию уровня безопасности ИТ-продукта как метод определения соответствия ИТ-продукта их запросам.** Обычно эти запросы составляются на основании результатов проведенного анализа рисков и выбранной политики безопасности. "Единые критерии" играют существенную роль в процессе формирования запросов потребителей, так как содержат механизмы, позволяющие сформулировать эти запросы в виде стандартизованных требований. Это позволяет потребителям принять обоснованное решение о возможности использования тех или иных продуктов. Наконец, "Единые критерии" предоставляют потребителям механизм Профилей защиты, с помощью которого они могут выразить специфичные для них требования, не заботясь о механизмах их реализации.

**Производители должны использовать "Единые критерии" в ходе проектирования и разработки ИТ-продуктов, а также для подготовки к квалификационному анализу и сертификации.** Этот документ дает возможность производителям на основании анализа запросов потребителей определить набор требований, которым должен удовлетворять разрабатываемый им продукт. Производители используют предлагаемую "Едиными критериями" технологию для обоснования своих претензий на то, что поставляемый ими ИТ–продукт успешно противостоит угрозам безопасности, на основании того, что он удовлетворяет выдвинутым функциональным требованиям и их реализация осуществлена с достаточным уровнем адекватности. Для осуществления этой технологии "Единые критерии" предлагают производителям специальный механизм, названный Проект защиты, дополняющий Профиль защиты и позволяющий соединить описания требований, на которые ориентировался разработчик, и спецификации механизмов реализации этих требований.

**Эксперты по квалификации используют этот документ в качестве основных критериев определения соответствия средств защиты ИТ–продукта требованиям, предъявляемым к нему потребителями и угрозам, действующим в среде его эксплуатации.** "Единые критерии" описывают только общую схему проведения квалификационного анализа и сертификации, но не регламентируют процедуру их осуществления. Вопросам методологии квалификационного анализа и сертификации посвящен отдельный документ – "Общая методология оценки безопасности информационных технологий".

Таким образом, "Единые критерии" обеспечивают нормативную поддержку процесса выбора ИТ–продукта, к которому предъявляются требования функционирования в условиях действия определенных угроз, служат руководящим материалом для разработчиков таких систем, а также регламентируют технологию их создания и процедуру оценки обеспечиваемого уровня безопасности.

"Единые критерии" рассматривают информационную безопасность, во–первых, как совокупность конфиденциальности и целостности информации, обрабатываемой ИТ–продуктом, а также доступности ресурсов ВС (вычислительной системы), и, во–вторых, ставят перед средствами защиты задачу противодействия угрозам, актуальным для среды эксплуатации этого продукта и реализации политики безопасности, принятой в этой среде эксплуатации.

"Единые критерии" регламентируют все стадии разработки, квалификационного анализа и эксплуатации ИТ–продуктов используя схему уже знакомую нам по "Федеральным критериям". "Единые критерии" предлагают достаточно сложную и бюрократичную концепцию процесса разработки и квалификационного анализа ИТ–продуктов, требующую от потребителей и производителей огромного количества работы по составлению и оформлению весьма объемных и подробных нормативных документов. Коротко рассмотрим основные положения и разделы этих документов, но сначала введем определения для некоторых базовых понятий "Единых критериев":

Задачи защиты – базовое понятие "Единых критериев", выражающее потребность потребителей ИТ–продукта в противостоянии заданному множеству угроз безопасности или в необходимости реализации политики безопасности.

Профиль защиты – специальный нормативный документ, представляющий собой совокупность Задач защиты, функциональных требований, требований адекватности и их обоснования. Служит руководством для разработчика ИТ–продукта при создании Проекта защиты.

Проект защиты – специальный нормативный документ, представляющий собой совокупность Задач защиты, функциональных требований, требований адекватности, общих спецификаций средств защиты и их обоснования. В ходе квалификационного анализа служит в качестве описания ИТ–продукта.