Н. М. Никифорова

АНАЛИТИЧЕСКИЙ ОБЗОР КРИТЕРИЕВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ВЕДУЩИХ ЗАРУБЕЖНЫХ СТРАН (США, КАНАДА, ЕВРОПЕЙСКИЙ СОЮЗ)

Критерии безопасности компьютерных систем (TCSEK-Trusted Computer System Evaluation Criteria) впервые были сформулированы разработчиками Министерства обороны США в 1983 г. в документе, получившем название «Оранжевая книга» (по цвету издания). Концепции и функциональные требования, сформулированные в нем, стали основой и ориентиром для разработки появившихся впоследствии иных стандартов безопасности. Так, впервые было дано определение безопасной компьютерной системы как системы, поддерживающей управление доступом к обрабатываемой в ней информации таким образом, что только авторизованные пользователи или процессы, действующие от их имени, имеют возможность читать, создавать, редактировать и удалять информацию.

В «Оранжевой книге» были предложены три критерия безопасности, а именно: политика безопасности, аудит и корректность, а в рамках этих критериев были сформулированы шесть базовых требований безопасности, такие как политика безопасности (доступ субъекта к объекту возможен только на основе идентификации и набора правил доступа), метки (атрибуты контроля доступа, соответствующие конкретным объектам), идентификация и аутентификация (обязательность наличия у субъектов уникальных идентификаторов, проходящих процедуру подтверждения подлинности), регистрация и учет (отслеживание значимых с точки зрения безопасности событий в системе, сопутствующий анализ потока событий, регистрация их в защищенном протоколе, определение степени ответственности пользователей), контроль корректности функционирования средств защиты (все средства защиты, обеспечивающие вышеупомянутые требования, должны контролироваться не зависимыми от них средствами контроля корректности функционирования) и непрерывность защиты (в течение всего цикла жизни компьютерной системы все средства защиты должны быть непрерывно и постоянно защищены от несанкционированных вмешательства или отключения, а также от этих угроз, действующих совместно).

Все системы по «Оранжевой книге» разделялись на семь классов защиты (от D до A в порядке возрастания защищенности), которые рекомендовалось выбирать на основе одного из пяти определенных предполагаемых режимов функционирования системы (режимы изолированной безопасности, контролирующий, многоуровневый, особой секретности и режим, в котором система непрерывно обрабатывает информацию одного класса в обеспечивающем безопасность для работы с ним окружении) и с учетом индекса риска (т. е. разности между максимальным классом информации и минимальным классом пользователей).

«Оранжевая книга» представляла собой первую попытку создания единого для разработчиков, потребителей и специалистов по сертификации стандарта безопасности. Однако специфика разработки документа, рассчитанного преимущественно на компьютерные системы военного назначения (причем в основном на операционные системы) привела к излишнему доминированию требований по обеспечению конфиденциальности информации и исключению возможностей ее разглашения и одновременно к недостаточной проработанности аспектов адекватности реализации средств защиты и политики безопасности. Указанная специфика лежит и в основе того факта, что, по мнению большинства специалистов, в настоящее время такие показатели рассмотренного стандарта, как универсальность (применимость к большому числу типов систем и областей информационных технологий), гибкость (возможность применения к развивающимся технологиям)

и гарантированность (определяемая мощностью предусмотренных стандартом методов и средств подтверждения надежности результатов анализа) находятся на ограниченном уровне, т. е. при применении этого стандарта возникают довольно значительные трудности.

Упомянутые недостатки «Оранжевой книги», а также анализ опыта ее использования были среди причин, которые побудили специалистов Национального института стандартов и технологий США и Агентства национальной безопасности США к разработке в 1992 г. **Федеральных критериев безопасности информационных технологий** (Federal Criteria for Information Technology Security), в настоящее время являющихся одной из составляющих Американского федерального стандарта по обработке информации.

Среди целей создания данного документа были разработка основных универсальных базовых требований к безопасности современных информационных технологий, совершенствование уже существующих требований и критериев, приведение к некоему общему соответствию принятых в разных странах критериев и требований безопасности информационных технологий, а также закрепление основополагающих принципов информационной безопасности в нормативном виде.

Федеральные критерии имеют своими объектами как продукты информационных технологий (т. е. некие предоставляемые конечному потребителю совокупности программных и аппаратных средств, а также совокупности указанных составляющих в отдельности), так и системы обработки информации (разработанные для решения определенных прикладных задач в конкретных средах эксплуатации, в отличие от общих сред эксплуатации в случае продукта информационных технологий). В то же самое время определения и нормы документа относятся к отдельным продуктам информационных технологий (оставляя «за скобками» вопросы построения систем обработки информации из совокупности составляющих) и затрагивают только аспекты механизмов встроенной (в виде специальных, аппаратных, программных средств) защиты, т. е. собственных средств обеспечения безопасности продуктов информационных технологий.

Основным понятием Федеральных критериев безопасности является понятие профиля защиты (Protection Profile) как нормативного документа, определяющего и обосновывающего состав и содержание средств защиты, устанавливающего требования к технологии разработки и квалификационному анализу. Профиль защиты, как правило, описывает некоторую совокупность близких по характеристикам продуктов информационных технологий и состоит из таких разделов, как описание, обоснование, функциональные требования к продукту, требования к технологии разработки продукта и требования к процессу квалификационного анализа продукта.

Процесс разработки информационных систем, представленный в Федеральных критериях, начинается с формулирования требований заказчиками и оканчивается введением системы в эксплуатацию. Этот процесс разбит на этап разработки и анализа профиля защиты, этап разработки и квалификационного анализа ИТ-продукта и этап компоновки и сертификации системы обработки информации в целом. Однако детально Федеральные критерии регламентируют только первый из вышеуказанных этапов, остальные два находятся за пределами рассмотрения этого стандарта.

В настоящее время отраслевые эксперты оценивают рассмотренный стандарт безопасности как имеющий высокий уровень универсальности, отличную гибкость и достаточную гарантированность.

Канадские критерии безопасности компьютерных систем (Canadian Trusted Computer Product Evaluation Criteria) были разработаны в 1993 г. специалистами из Центра безопасности ведомства безопасности связи Канады (Canadian System Security Centre Communication Security Establishment). В разработанном документе чувствуется сильное влияние «Оранжевой книги» и Федеральных критериев безопасности. Однако, в отличие, например, от первого упомянутого документа (который, как говорилось выше, рассчитывался на применение в отношении

операционных систем), Канадские критерии изначально были нацелены на широкий диапазон компьютерных систем. Целями были разработка единой шкалы критериев для возможности сравнения различных систем обработки информации по степени безопасности, создание основы для разработки спецификаций безопасных компьютерных систем (которая могла бы использоваться разработчиками при проектировании подобных систем в качестве руководства для определения состава функций средств защиты) и, наконец, разработка унифицированного подхода и стандартных средств для описания характеристик безопасных компьютерных систем.

По своей структуре Канадские критерии безопасности состоят из функциональных требований к средствам защиты и требований к адекватности их реализации.

Функциональные критерии представлены четырьмя группами — критерии конфиденциальности, критерии целостности, критерии работоспособности и критерии аудита.

Первый из этих критериев описывает средства, которые призваны устранить угрозы несанкционированного доступа к информации. Это контроль скрытых каналов, произвольное управление доступом, нормативное управление доступом, повторное использование объектов. Второй критерий устанавливает требования к средствам, противостоящим угрозам несанкционированного изменения или искажения информации (это критерии доменов целостности, физической целостности, разделения ролей, самотестирования и т. д.). Третий критерий устанавливает требования к средствам, обеспечивающим защиту от угроз нарушения доступности. Раздел аудита призван обеспечить противодействие угрозам фальсификации протоколов и манипуляций с внутрисистемной информацией и включает в себя регистрацию и учет событий в системе, идентификацию и аутентификацию, а также прямое взаимодействие с ядром безопасности.

Адекватность реализации в Канадских критериях определяется тем, насколько точно и последовательно средства защиты следуют политике безопасности компьютерной системы, т. е. правилам, установленным для обработки, хранения и использования информации в системе. Уровень адекватности присваивается всей системе в целом.

Таким образом, в общем случае Канадские критерии оценивают степень безопасности исходя из совокупности функциональных возможностей защиты (описанных в четырех перечисленных разделах функциональных требований) и одного обобщенного параметра — уровня адекватности, уделяя большое внимание взаимному соответствию и взаимодействию всех систем и средств обеспечения безопасности.

В Канадских критериях, как и в Федеральных критериях, не принимается подход к оценке уровня безопасности с помощью некоторой универсальной шкалы, а используется независимое ранжирование требований в разделах по целому ряду различных критериев, каждый из которых характеризует работу конкретной подсистемы безопасности. Качество же обеспечения безопасности всей системы в целом характеризуется уровнем адекватности реализации политики безопасности.

Наряду с рассмотренными национальными стандартами были созданы и международные стандарты, такие как **Европейские критерии безопасности информационных технологий** (Information Technology Security Evaluation Criteria), разработанные организациями стран Европейского союза: Агентством информационной безопасности (Германия), Агентством национальной безопасности коммуникаций (Нидерланды), Органом исполнения программ безопасности и сертификации ИТ (Англия) и Центром обеспечения безопасности систем (Франция). Разработанные в 1991 г. Европейские критерии самым тесным образом были связаны с «Оранжевой книгой», что, по мнению некоторых специалистов, делает их не вполне самостоятельным документом. Хотя, с другой стороны, требование адекватности средств защиты было впервые введено именно в Европейских критериях для определения степени уверенности в правильности выбора и надежности функционирования избранного набора реализуемых функций безопасности (таких как идентификация и аутентификация, восстановление после сбоев, управление доступом, целостность информации и т. д.).

В настоящее время эти европейские стандарты не слишком актуальны, но они совместно с Федеральными критериями и Канадскими критериями стали основой для самого употребляемого в настоящий момент европейского стандарта 1999 г. — **Общих критериев безопасности информационных технологий** (Common Criteria for Information Technology Security Evaluation).

Разработка этого документа была начата в июне 1993 г. специалистами, участвовавшими в разработке Европейских, Федеральных и Канадских критериев. Сегодня версия 2.1 данного стандарта утверждена Международной организацией по стандартизации в качестве международного стандарта информационной безопасности ISO/IEC 15408. Можно достаточно уверенно говорить о том, что Общие критерии являются наиболее целостным, проработанным и совершенным стандартом в настоящее время.

При разработке этих стандартов информационной безопасности целью было удовлетворение запросов и согласование позиций производителей и потребителей, а также экспертов по безопасности в процессе создания и эксплуатации продуктов информационных технологий.

Производители используют Общие критерии при проектировании и разработке, поэтому от стандартов им необходима максимальная по уровню конкретность, а также совместимость требований стандартов с современными средствами и технологиями обработки информации и с распространенными операционными системами. Для экспертов этот документ необходим при определении соответствия средств защиты требованиям, которые предъявляются к ним (в первую очередь потребителями), и действующим угрозам. Для большинства потребителей наибольшее значение имеют простота установленных критериев безопасности и однозначность параметров выбора защищенной системы, а для другой части пользователей немалую роль играет возможность применения критериев к достаточно специфическим продуктам информационных технологий.

Общие критерии устанавливают нормы для всех стадий разработки, квалификационного анализа, эксплуатации всех продуктов информационных технологий, при этом используя заимствованную из Федеральных стандартов схему. Действуя в ее рамках, потребители и производители должны проводить большую работу по составлению и оформлению объемных отчетных документов.

Аналогично Федеральным критериям, разработчики отказались от единой шкалы безопасности и ввели достаточное количество гибких инструментов, позволяющих реализовывать дополнительные возможности по выбору конкретных требований и адаптации их к необходимым прикладным задачам. Немалое значение придается и адекватности функциональных требований, обеспечиваемой независимым анализом и тестированием продукта, а также применением специальных технологий на всех этапах проектирования и разработки.

Используя упомянутые выше показатели универсальности, гибкости и гарантированности, можно сказать, что Общие критерии удовлетворяют им в превосходной степени. Универсальность заключается в том, что в настоящее время технология создания любого ИТ-продукта включает в себя обязательное использование стандарта. Гибкость выражается, например, в возможности для потребителей сформулировать свои требования с помощью механизма профилей защиты, а для производителей — продемонстрировать, как эти требования реализуются на практике. Гарантированность реализации защиты в Общих критериях — это самый важный компонент информационной безопасности, предусматривающий многоэтапный контроль на каждой стадии разработки продукта, учитывающий соответствие результатов начальным целям путем доказательства адекватности защиты принятым требованиям.

Общие критерии удовлетворяют всем требованиям актуальности, поскольку предлагают механизмы удовлетворения нужд пользователей (профиль защиты, проект защиты) и позволяют адаптировать технологию создания информационных систем к новым требованиям. Наличие же в Общих критериях большого количества функциональных требований (135 требований) дает возможность для качественной разработки защищенных систем.

В качестве резюме можно сказать следующее:

1) в результате развития и критического анализа предлагаемых стандартов произошел отказ от единой шкалы критериев в пользу введения большого числа независимых показателей и упорядоченных шкал,

2) требования адекватности реализации защиты приобретают все более важное значение,

3) стандарты безопасности стали неотъемлемой частью всей сферы информационных технологий, определив роли производителей, потребителей и экспертов и разделив их функции,

4) состоявшееся на основе стандартов «разделение ролей» участников процесса создания и эксплуатации защищенных систем привело к соответствующему распределению ответственности,

5) и, наконец, стандарты информационной безопасности приобрели международную важность и значение.