Ирина БАЛИНА,
Славянский университет Республики Молдова

ОБЩИЕ КРИТЕРИИ И МЕТОДОЛОГИЯ БЕЗОПАСНОСТИ IT-ТЕХНОЛОГИЙ. МЕЖДУНАРОДНЫЕ СОГЛАШЕНИЯ

It investigates formation features of general Informational Technology (IT) security methodology, perspectives and strategies of their international development. It examines password protection example as quantative mark criterion of security mechanisms.

Построение всеохватывающей системы информационной безопасности, минимизация рисков – процесс весьма сложный, длительный и дорогостоящий. В мире нет ни одной организации, которая внедрила бы весь набор средств и реализовала все необходимые, описанные в стандартах, процессы. Выбор подходящих методов и степени защиты является субъективным процессом, лишь отчасти регламентируемым нормативными актами.

Целью данной работы является исследование особенностей формирования общей методологии безопасности IT-технологий, перспектив и стратегии их международного развития.

Метод сбора данных – мониторинг материалов аналитических обзорных статей в СМИ и глобальной сети Internet, анализ международных стандартов в области IT-безопасности.

Метод анализа данных – традиционный контент-анализ документов.

Работы по созданию международного стандарта (исторически сложившееся название "Общие критерии") в области оценки IT-безопасности информационных технологий были развернуты под эгидой Международной организации по стандартизации (ИСО) при содействии в дальнейшем государственных организаций США, Канады, Великобритании, Франции, Германии и Нидерландов и преследовали следующие **основные цели**:

- *унификацию национальных стандартов в области оценки IT- безопасности;*
- *повышение уровня доверия к оценке IT-безопасности;*
- *сокращение затрат на оценку IT-безопасности на основе взаимного признания сертификатов.*

Официальный текст международного стандарта ISO/IEC 15408 издан 1 декабря 1999 года. Изменения, внесенные в стандарт на завершающей стадии его принятия, учтены в версии 2.1 Общих критериев (ОК), идентичной стандарту по содержанию. В 2002 году на основе аутентичного текста ISO/IEC 15408 был принят российский стандарт ГОСТ Р ИСО/МЭК 15408-2002 "Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий".

В поддержку стандарта под эгидой ИСО разработан целый ряд нормативно-методических документов. Среди них:

- Руководство по разработке профилей защиты и заданий по безопасности;
- Процедуры регистрации профилей защиты;
- Общая методология оценки безопасности информационных технологий (ОМО).

Основным лейтмотивом создания ОМО явилась унификация на международном уровне способов и приемов проведения оценки по ОК в целях взаимного признания оценок и, таким образом, устранения накладных расходов, связанных с дублированием оценок продуктов IT и профилей защиты.

Взаимное признание оценок (The International Mutual Recognition Arrangement – MRA), полученных на основе Общих критериев, регламентируется соглашением правительственных организаций Канады, Франции, Германии, Великобритании и США, в соответствии с которым стороны обязуются признавать сертификаты на продукты и системы IT, полученные в странах, присоединившихся к Соглашению, если они получены на основе применения Общих критериев и выданы организациями, удовлетворяющими требованиям Соглашения. Установленные в MRA правила позволяли присоединиться к Соглашению как в виде участника, только признающего сертификаты, выданные в соответствии с ОК, так и в виде участника, выдающего эти сертификаты.

В мае 2000 года представителями уже четырнадцати стран (Канады, Франции, Германии, Великобритании, США, Нидерландов, Италии, Греции, Испании, Швеции, Норвегии, Финляндии, Австралии и Новой Зеландии) было подписано более универсальное (по сравнению с MRA) соглашение CCRA (Arrangement of the Recognition of Common Criteria Certificates in the field of Information Technology Security). Соглашение CCRA значительно расширяет возможности присоединения новых стран-участниц. В последующем к соглашению CCRA присоединился Израиль, Австрия, Турция, Венгрия и Япония.

В настоящее время общеупотребительным подходом к построению критериев оценки безопасности IT является использование совокупности определенным образом упорядоченных

качественных требований к функциональным механизмам обеспечения безопасности, их эффективности и доверия к реализации. Несмотря на это, ОМО предусматривает возможность проведения там, где это применимо, количественных оценок с использованием соответствующих качественных показателей. При этом количественные критерии целесообразно использовать для оценки таких механизмов безопасности, как парольная защита, контрольное суммирование и т.п. Рассмотрим пример анализа стойкости функции безопасности (СФБ) для гипотетического механизма цифрового пароля. Предполагается, что пароли состоят не менее чем из четырех символов, являющихся цифрами. Все цифры должны быть различны. Кроме того, запрещается использовать "явно неслучайные" пароли, представляющие собой последовательно возрастающие или убывающие совокупности цифр (1234, 8765 и т.п.), и не должны быть связаны каким-либо способом с конкретным пользователем, например, с датой рождения. В среднем нарушитель должен был бы ввести 2513 цифровых комбинаций до ввода правильного цифрового пароля. Как результат, в среднем, успешное нападение произошло бы чуть меньше, чем за **2513 мин / (60 мин/час) ~ 42 часа**

Число возможных значений цифровых паролей рассчитывается следующим образом:

1.Допуская самый плохой вариант сценария, когда пользователь выбирает число, состоящее только из четырех цифр, число перестановок цифрового пароля (предполагая, что каждая цифра уникальна) равно: $7 \times 8 \times 9 \times 10 = 5040$

2.Число возможных увеличивающихся рядов – семь, как и число убывающих рядов. После отбрасывания этих рядов число возможных значений цифровых паролей равно: $5040 - 14 = 5026$

Основываясь на дополнительной информации в механизме цифрового пароля, целесообразно использовать характеристику блокировки терминала. После шестой подряд неудачной попытки аутентификации терминал блокируется на один час. Счетчик неудачной аутентификации сбрасывается через пять минут; таким образом, нарушитель в лучшем случае может осуществить **пять попыток ввода цифрового пароля каждые пять минут или 60 вводов цифрового пароля в час.**

С использованием Общих критериев (ОК) можно провести анализ технологий и продуктов на основе типовых методик оценки ОМО и представлять их в виде сетевых моделей (Е-сетей). Например, типовые методики сертификационных испытаний по Общим критериям используются при сертификации межсетевого экрана "Z-2" (разработчик – ЗАО "Инфосистемы Джет"), операционной системы Microsoftndows Professional Service Pack 1a (разработчик – корпорация Microsoft), межсетевого экрана Symantec(TM) Enterprice Firewall, Version 7.0.4 (разработчик – корпорация Symsntec). Таким образом, имея сетевое представление большинства из используемых пакетов доверия и разработав правила корректной композиции этих сетевых представлений, мы можем в короткие сроки разрабатывать рабочие программы и методики оценки продуктов и систем IT, эффективно применять Общие критерии ОМО при сертификации продуктов и систем IT.

В настоящее время именно ОК/ОМО версии 3.0 планируется как основа нового издания стандарта ИСО, а также как официальные документы Соглашения CCRA. При этом отметим, что в ОМО рассмотрены не все вопросы, связанные с оценкой безопасности IT, и это обуславливает необходимость дальнейшей разработки дополнительных руководств для всех участников оценки: заявителей, разработчиков, испытательных лабораторий и органа по сертификации, а также руководства по сопровождению сертификатов соответствия продуктов и систем IT требованиям безопасности информации.

Литература:

1. *Information technology – Security techniques – Evaluation Criteria for IT Security. Part 1: Introduction and general model*. ISO/IEC 15408-1.
2. ГОСТ Р ИСО/МЭК 15408-2-2002. *Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий*. Часть 2: Функциональные требования безопасности.
3. Г. А. Черней, С. А. Охрименко, Ф. С. Ляху. *Безопасность автоматизированных информационных сетей*. Ruxanda, 1996.