УДК 65.012:34(477)

М.В. Цуранов, А.В. Слипченко

Харьковский национальный университет внутренних дел, Харьков

ИСПОЛЬЗОВАНИЕ КОМПЛЕКСНЫХ ПОКАЗАТЕЛЕЙ ПРИ РАЗРАБОТКЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ

В статье рассмотрен комплексный показатель эффективности использования операционной системы, включающий оценку эффективности подсистемы информационной безопасности.

Ключевые слова: *операционная система, показатель эффективности, информационная безопасность.*

Вступление

В последнее время особую роль для государственных и коммерческих организации играет эффективное использование существующих у нее информационных ресурсов. В этом случае ключевое значение получает информационная инфраструктура организации, в которой обычно выделяют техническое, программное и организационное обеспечение.

В связи со сложным финансовым положением большинство пользователей в нашей стране привыкли использовать не лицензированные операционные системы (ОС), при этом пользователи забывают, что за взломом стоит существенное изменение внутреннего кода ОС. Изменение кода влечет за собой возможное появления троянских программ уже сразу при установке ОС, исходя из этого, никто не может гарантировать уровень безопасности такой системы.

Путем различного рода манипуляций с ОС злоумышленникам нередко удается получать значительные суммы денег, уклоняться от налогообложения, заниматься промышленным шпионажем, уничтожать программы конкурентов и т.д.

Однако, даже использование лицензионного программного обеспечения (ПО) не дает нам возможности оценить его эффективность и экономический эффект от его внедрения.

Цель статьи: разработать комплексный показатель эффективности ОС для анализа их уровня защищенности.

Изложение основного материала

Для решения проблемы оценки уровня защищенности ОС были разработаны многочисленные стандарты безопасности [1 – 3]. Однако дальнейший анализ стандартов показал что в большинстве из них модель нарушителя и модель угроз строится производителем ОС [4]. Такой подход не позволяет достоверно оценить уровень информационной безопасность (ИБ). Это объясняется тем, что разработчик для повышения уровня сертификата преднамеренно составляет модель с минимальным, часто не соответствующим реалиям, количеством угроз. Поэтому стандарты безопасности не дают реальной количественной оценки эффективности средств защиты ОС.

Большинству руководителей и администраторов безопасности необходима количественная оценка уровня безопасности ОС, наиболее полно это можно сделать используя комплексные показатели эффективности.

В специальной литературе можно встретить следующее определение показателя эффективности - количественная характеристика свойства эффективности системы или целеустремленного процесса, которая является результатом измерения или подсчета[5]. Для того, чтобы более полно оценить эффективность систем нужно решать многокритериальные задачи.

Под критерием эффективности следует понимать - правило или способ принятия решения с учетом эффективности системы.

Проведенный анализ общих критериев эффективности информационных технологий показал, что наиболее полезными с социальной точки зрения для общества являются те информационные технологии, которые позволяют сэкономить наибольшее количество социального времени, высвобождая его для других целей, в том числе — для целей развития общества [6]. В работе [6] были выделены основные принципы проектирования высокоэффективных технологий, а именно: концентрация ресурсов в пространстве, концентрация ресурсов во времени, векторная ориентация ресурсов.

Для оптимизации и количественной оценки эффективности возможных вариантов проектируемых или же уже существующих информационных технологий необходимо правильно выбирать критерии их эффективности [7].

Важность правильного выбора данных критериев обусловлена необходимостью оптимизации и количественной оценки эффективности возможных вариантов проектируемых или же уже существующих информационных технологий. Такими критериями являются функциональные и ресурсные.

Функциональные критерии, значения которых характеризуют степень достижения при данной технологии тех желаемых характеристик информационного процесса, которые необходимы пользователю. Такими характеристиками могут быть, например [8]:

- объемно-временные характеристики реализуемого информационного процесса (скорость передачи данных, объем памяти для хранения информации и т. п.);
- надежностные характеристики реализации информационного процесса (вероятность правильной передачи или преобразования информации, уровень ее помехозащищенности и др.):
- параметрические характеристики, описывающие степень достижения основного конечного результата информационного процесса, реализуемого при помощи данной технологии (правильность распознавания речи или изображения, качество формируемой графической информации и др.).

Ресурсные критерии эффективности позволяют принципиально сравнивать между собой различные виды технологий. Кроме того, они дают возможность количественно оценить получаемый в результате применения этих технологий эффект с точки зрения их социальной полезности в плане экономии различных видов ресурсов общества[8].

Анализ эффективности использования ОС основан на расчете фондоотдачи и фондоемкости. Установлено, что для разработки технологической политики предприятия необходим углубленный факторный анализ данных показателей [7].

Для того чтобы оценить эффективность современных ОС не достаточно одного показателя, поэтому необходимо вводить комплексный показатель эффективности с весовыми коэффициентами для учета влияния показателя на общую эффективность ОС.

Весовой коэффициент — числовой коэффициент, параметр, отражающий значимость, относительную важность, «вес» данного фактора, показателя в сравнении с другими факторами, оказывающими влияние на изучаемый процесс[5].

Для объективной количественной оценки эффективности средств защиты ОС, с учетом требований предъявляемыми руководителями фирм и администраторами безопасности авторы предлагают использовать следующий комплексный показатель:

$$К_э = k_1 \frac{К_{вс}}{Квел} + k_2 К_{ди} + k_3 \frac{Квос}{Квоб} + \\ + k_4 К_{ксб} + k_5 К_{экспл} + k_6 К_{ауд},$$

где $\frac{К_{вс}}{Квел}$ – показатель взаимной совместимости программного обеспечения для различных ОС, в числители количество используемых программ поддерживающие оцениваемую ОС, в знаменателе общее количество используемых программ ;

$К_{ди}$ – показатель дружественности интерфейса ОС;

$\frac{Квос}{Квоб}$ – показатель количества вирусов, в знаменателе общее количество вирусов в числителе количество вирусов для рассматриваемой ОС;

$К_{ксб}$ – показатель зарегистрированных сбоев в ОС;

$К_{экспл}$ – показатель стоимости эксплуатации ОС;

$К_{ауд}$ – показатель аудита, наблюдаемости ОС;

$k_1 \dots k_6$ – весовые коэффициенты.

Взаимная совместимость является важнейшим фактором, поскольку пользователи привыкают к единообразию интерфейса каждой из ОС. Переход на другую ОС, или другую версию, с кардинально измененным интерфейсом может потребовать значительных временных затрат на изучение новых принципов работы с интерфейсом. Исходя из этого, необходимо отметить, что от качественного взаимодействия интерфейсов разных ОС зависит производительность работы фирмы. Взаимная совместимость также подразумевает совместимость прикладного программного обеспечения между различными версиями и платформами ОС. С точки зрения безопасности взаимная совместимость подразумевает использование типичных средств ИБ.

Дружественный интерфейс играет большую роль в обучении персонала, поскольку пользователи привыкают к единообразию графических оболочек на домашних ПК и им будет достаточно сложно обучаться новым принципам работы с интерфейсом. Это повлечет дополнительные временные и финансовые затраты. Данный показатель особо следует учитывать при обновлении версий программного обеспечения, в случае если новая версия обладает измененным интерфейсом.

Все современные ОС подвержены вирусным атакам. Вирусы, даже при наличии антивирусных программ, способны значительно снизить производительность ПК и увеличить время, затрачиваемое на плановое обслуживание техники. Чем выше количество вирусов для ОС, тем выше вероятность заражения и дорогостоящего восстановления работоспособности ПК.

При выборе ОС или ее обновлении необходимо учитывать количество зарегистрированных в службе поддержки сбоев. На первоначальном этапе эксплуатации любая ОС обладает повышенным количеством сбоев, поэтому следует отдать предпочтение системам, которые коммерчески эксплуатируются на протяжении нескольких месяцев. Это значительно уменьшит количество сбоев и время простоя ПК, а также количество угроз в системе безопасности.

Важным параметром для любой ОС является стоимость ее эксплуатации, поскольку даже для бесплатных систем она может достигать значительных сумм. В данном параметре также необходимо рассматривать стоимость эксплуатации систем защиты ОС.

Для ИБ ОС наиболее важным параметром является наблюдаемость ОС или аудит, от наличия и развитости средств аудита зависит возможность раннего выявления угроз и недопущение их повторения.

Выводы

При выборе ОС руководители сталкиваются со значительной проблемой, какой ОС отдать предпочтение. Существующие стандарты и методики оценки качества ОС не могут дать однозначный количественный ответ на этот вопрос. Для устранения данного недостатка авторами предлагается использовать комплексный показатель эффективности ИБ ОС, который учитывает различные факторы, влияющие на характеристики защищенности.

Список литературы

1. Общие критерии оценки защищённости информационных технологий.[Электронный ресурс]. – Режим доступа: ru.wikipedia.org/wiki/Common_Criteria.

2. Международные стандарты информационной безопасности [Электронный ресурс]. – Режим доступа: http://ypn.ru/177/international-standards-of-information-technologies-security.

3. Шкала рейтингов международных стандартов информационной безопасности [Электронный ресурс]. – Режим доступа: www.cresit-rating.ua/ru/about-rating/ scale/12978.

4. Слипченко О.В. Стандарты безопасности операционных систем / О.В. Слипченко, М.В. Цуранов // Системи обробки інформації. Збірник наукових праць. Вип. 4(102). – Харків, ХУПС, 2012. – С. 78 -81.

5. Надежность и эффективность в технике: Справочник: В10 т. / Ред. совет: В.С. Авдуевский (пред.) и др. – М.: Машиностроение, 1986. Т. 1: Методология. Организация. Терминология/Под ред. А.И. Рембезы. – 224 с.

6. Проблема эффективности ресурсов информационных систем [Електронний ресурс]. – Режим доступу :http://kmt.stu.ru/mashukov/posob/htm_inf_men/gl8.htm.

7. Оценка эффективности информационных систем [Електронний ресурс]. – Режим доступу до ресурсу: http://www.ibm.com/developerworks/ru/library/l-otcenka_ efectivnosti_1/index.html.

8. Качество и эффективность информационных систем [Електронний ресурс]. – Режим доступу до ресурсу: http://www.rus-lib.ru/book/38/men/21/2.5.html.

Поступила в редколлегию 19.04.2013

Рецензент: д-р техн. наук, проф. А.А. Серков, Национальный технический университет «ХПИ», Харьков.

ВИКОРИСТАННЯ КОМПЛЕКСНИХ ПОКАЗНИКІВ ПРИ РОЗРОБЦІ ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ

М.В. Цуранов, О.В. Сліпченко

У статті розглянуто комплексний показник ефективності використання операційних систем, що включає оцінку ефективності підсистеми інформаційної безпеки.

Ключові слова: *операційна система, показник ефективності, інформаційна безпека.*

USING COMPLEX INDICATORS FOR SOFTWARE DEVELOPMENT

M.V. Tsuranov, O.V. Slipchenko

The article presents a comprehensive indicator of the effectiveness of the operating system, including the evaluation of the effectiveness of information security subsystem.

Keywords: *operating system, performance indicator, information security.*