УДК 004.451

ОЦЕНКА ЗАЩИЩЕННОСТИ ОПЕРАЦИОННОЙ СИСТЕМЫ

Мурадов Э.К., магистрант гр. 067241

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Петров С.Н. – канд. техн. наук

Аннотация. Представлены основные критерии для оценки защищенности операционной системы.

Ключевые слова. Информационная безопасность, операционная система, оценка защищенности.

Операционную систему (ОС) называют защищенной, если в ней реализованы средства защиты от основных классов угроз [1]. На основе данного определения, а также современных рекомендаций в области защиты информация, к основным оценочным критериям защищенности операционной системы можно отнести следующие.

1 Разграничение доступа к ресурсам системы и данным пользователей. В том числе возможность разграничения на разных уровнях.

2 Аутентификация, авторизация и идентификация пользователя при входе в систему, запросе доступа к ресурсу или данным.

3 Противодействие преднамеренному или случайному выводу из строя ОС или ее компонентов, в том числе установленного программного обеспечения.

4 Возможность использования шифрования данных пользователей и конфигураций системы.

5 Возможность ведения журнала событий, как действий пользователей и администраторов системы, так и событий самой системы и ее компонентов, для дальнейшего аудита.

6 Внедрение политик безопасности, в том числе дальнейшее управления ими.

7 Резервирование данных пользователя и конфигураций системы, в том числе с поддержкой шифрования таких данных.

Сетевое взаимодействие также должно контролироваться операционной системой. ОС должна определять, какое программное обеспечение и как использует сетевые возможности, журналировать события использования программным обеспечением сетевых ресурсов и при необходимости ограничивать взаимодействие с сетью.

Оценка защищенности должна учитывать архитектуру построения операционной системы. В случае комплексной архитектуры ОС должна иметь защищенные точки расширения функционала ядра системы для реализации отсутствующих средств обеспечения безопасности. В случае архитектур с модульным ядром или несколькими микроядрами необходимо обеспечение безопасных протоколов общения компонентов и отказоустойчивость фундаментальных сервисов.

При оценивании ОС необходимо производить испытание заявленных характеристик, в том числе анализировать предустановленные параметры для средств защиты информации. Такое тестирование может разделяться на активное и пассивное. Под активным тестированием подразумевается эмуляция действий потенциального злоумышленника по преодолению механизмов защиты, в том числе используя уязвимости разного уровня критичности. Положительным результатом тестирования считается отсутствие удачных попыток получить доступ к системе, данным в ней, а также отсутствие отказов в работе ОС и ее компонентов. Под пассивным тестированием подразумевается анализ конфигурационных файлов ОС, ее компонентов и установленного в базовой поставке программного обеспечения. Положительным результатом такого тестирования будет отсутствие уязвимостей, связанных с недостаточной настройкой объекта тестирования.

В качестве дополнительных критериев оценки предлагаются следующие:

1 Доступность исходного кода ОС и всех ее компонентов для изучения и анализа. Открытый исходный код позволяет быстрее обнаруживать критические и важные уязвимости, а также исправлять уже найденные.

2 Частота поставки стабильных обновлений для ОС и ее компонентов. В том числе возможность устанавливать только обновления безопасности, содержащие исправление ошибок и устраняющие уязвимости.

3 Отношение обнаруженных уязвимостей ОС и ее компонентов за определенный период к устраненным. Данная метрика позволяет оценить скорость реагирования компании-владельца ОС на найденные уязвимости в ОС и ее компонентах.

4 Публичность раскрытия факта обнаружения уязвимости в ОС и ее компонентах со стороны компании-владельца ОС. Своевременное оповещение о найденной уязвимости позволит предпринять некоторые действия для предотвращения угрозы безопасности.

Список использованных источников:
1.Информационная безопасность / Шаньгин В.Ф. // М.: ИНФРА-М, 2011. – с. 174.

UDC 004.451

ASSESSMENT OF THE OPERATING SYSTEM SECURITY

Muradov E.K., Master Student of the group 067241

Belarusian State University of Informatics and Radioelectronics
Minsk, Republic of Belarus

Petrov S.N. – PhD

Annotation. The main criteria for assessing of the operating systems security are presented.

Keywords. Information security, operating system, security assessment.