УДК 65.012:34(477)

М.В. Цуранов, А.В. Слипченко

Харьковский национальный университет внутренних дел, Харьков

СТАНДАРТЫ БЕЗОПАСНОСТИ ОПЕРАЦИОННЫХ СИСТЕМ

В статье рассмотрены зарубежные стандарты безопасности операционных систем ISO/IEC 15408, ISO/IEC 17799:2002 (BS 7799:2000) и германский стандарт BSI, проведена сравнительная оценка эффективности их использования.

Ключевые слова: *системы международной сертификации, стандарты безопасности операционных систем, операционная система, модель угроз, модель нарушителя, ISO/IEC 15408, BSI.*

Вступление

Развитие компьютерной техники и ее широкое внедрение в различные сферы человеческой деятельности привело к расширению сферы использования операционных систем (ОС), которые стали хранить и обрабатывать значительные массивы конфиденциальных данных, что повлекло за собой рост противозаконных действий по отношению к системам. ОС можно встретить в: персональных компьютерах (ПК), планшетных ПК, мобильных телефонах, системах управления, системах сигнализации и других электронных устройствах. В связи со сложным финансовым положением большинство пользователей в нашей стране привыкли использовать не лицензированные 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.

В настоящее время существуют стандарты оценки безопасности ОС, при соответствии которым ОС получает сертификат который гарантирует определенный уровень защищенности. Одним из главных результатов стандартизации в сфере систематизации требований и характеристик защищенных информационных комплексов и ОС стала система международных и национальных стандартов безопасности информации, которая насчитывает более сотни различных требований и документов.

В работе [1] было проведено исследование в результате которого получены следующие данные: около 58% опрошенных пострадали от компьютерных взломов за последний год. Примерно 18% опрошенных из числа пострадавших заявляют, что потеряли более миллиона долларов в ходе нападений, более 66% потерпели убытки в размере 50 тыс. долларов. Свыше 22% атак были нацелены на похищение промышленных секретов или документов, представляющих экономический интерес.

Исходя из вышесказанного, оценка безопасности операционных систем – важнейший фактор при

© М.В. Цуранов, А.В. Слипченко

выборе программного обеспечения для фирм, учреждений и государства.

Цель статьи: провести анализ международных и национальных стандартов безопасности операционных систем.

Структура стандартов

Одним из способов оценки безопасности ОС являются стандарты, соблюдение которых дают определенную гарантию защищенности.

Основная проблема украинских стандартов безопасности ОС – это отсутствие своего стандарта безопасности ОС.

Следует сказать, что при использовании ОС в бизнесе и в государственном документообороте необходимо знать уровень их защищенности. Системы документооборота, базирующиеся на существующих ОС, чаще всего производятся в США или странах западной Европы. Следовательно они поставляются с сертификатами безопасности указанных выше стран, которые могут не соответствовать друг другу и существующим украинским нормативным документам.

Стандарты защиты данных, образуют базис понятий, на котором строятся все действия по обеспечению информационной безопасности (ИБ). В то же время стандарты ориентированы в первую очередь на производителей ПО и экспертов в области безопасности и в гораздо меньшей степени - на пользователей и администраторов.

Стандарты не учитывают уровень знаний обычного пользователя, поэтому ему сложно настроить защиту в соответствии с теми настройками, которые были применены при оценке соответствия ОС стандартам безопасности. В отличии от пользователя администратор, имеет все необходимые знания и возможность настроить ОС, однако для этого необходимо потратить много времени, что не всегда целесообразно. Проблема поставляемых в Украину ОС в том, что настройки их функций безопасности при инсталляции не соответствуют стандартам.

Стандарты статичны в том что:

1. Стандарты не описывают методических указаний по настройке функций защиты в ОС .

2. В стандартах невозможно учитывать возникающие угрозы при создании новых ОС (к примеру, версии ОС семейства Windows и Linux выходят каждые 2 года, а стандарты пересматриваются не чаще раза в 5 лет).

3. Не целесообразно создавать стандарты для каждой новой версии ОС, потому как на создание нового стандарта понадобится гораздо больше времени, чем на разработку новой версии ОС.

ИБ обеспечивается не только с помощью аппаратного и программного обеспечения, но в первую очередь работой с обслуживающим персоналом. Основным помощником на этом пути являются международные стандарты ИБ и менеджмента в сфере информационной безопасности, которые помогут определить уязвимые места в безопасности предприятия и возможные пути их устранения.

Основная цель стандартов [2]: обеспечить выполнение требований безопасности при создании или развитии информационной системы организации, поддерживать безопасность приложений и данных.

Анализ стандартов в области безопасности ОС. Существует несколько видов стандартов: международные, национальные и стандарты отдельных фирм. В данной статье будут рассмотрены только первые два вида стандартов, поскольку последний, в силу малого распространения, не представляет научного интереса. Любой стандарт безопасности предполагает наличие следующих этапов [2]:

1. Определение целей обеспечения ИБ компьютерных систем.
2. Создание эффективной системы управления ИБ.
3. Разработка критериев и показателей эффективности использования ОС с точки зрения обеспечения ИБ.
4. Расчет комплексного показателя ИБ для оценки соответствующей ОС.
5. Применение инструментария обеспечения ИБ и оценки ее текущего состояния.
6. Использование методик управления безопасностью с обоснованной системой метрик и мер обеспечения ИБ, позволяющих объективно оценить защищенность информационных активов.

Международный стандарт ISO/IEC 15408. 8 июня 1999 года был утвержден Международный стандарт ISO/IEC 15408 под названием "Общие критерии оценки безопасности информационных технологий". Общие критерии (ОК) обобщили содержание и опыт использования Оранжевой книги, развили европейские и канадские критериев, и воплотили в реальные структуры концепцию типовых профилей защиты федеральных критериев США. В ОК проведена классификация широкого набора требований безопасности информационных технологий, определены структуры их группирования и принципы использования.

Главные достоинства ОК[3] — полнота требований безопасности и их систематизация, гибкость в применении и открытость для последующего развития. Использование методик данного стандарта позволяет определить для компании те критерии, которые могут быть использованы в качестве основы для выработки оценок защитных свойств продуктов и систем информационной технологии. Кроме того, эти методики позволяют проводить наиболее полное сравнение результатов оценки защитных свойств корпоративных информационных систем с помощью общего перечня (набора) требований для

функций защиты продуктов и систем, а также методов точных измерений, которые проводятся во время получения оценок защиты.

Результаты оценок защиты позволяют определить для компании достаточность защиты корпоративной информационной системы. Вместе с тем в ОК главное внимание уделено защите от несанкционированного доступа (НСД).

Главный недостаток стандарта в том что ОК так и не удалось решить проблему НСД, модификации или потери доступа к информации в результате случайных или преднамеренных действий и ряд других аспектов ИБ. Еще один недостаток стандарта – модель нарушителя составляет разработчик ОС, следовательно он может не учесть все аспекты реального функционирования ОС.

Стандарты ISO/IEC 17799:2002 (BS 7799:2000). В настоящее время Международный стандарт ISO/IEC 17799:2000 (BS 7799-1:2000) “Управление информационной безопасностью – Информационные технологии. - Information technology- Information security management” является наиболее известным стандартом в области защиты информации.

Текущая версия стандарта ISO/IEC 17799:2000 (BS 7799-1:2000) рассматривает следующие актуальные вопросы обеспечения ИБ организаций и предприятий[4]:

1. Необходимость обеспечения ИБ.
2. Основные понятия и определения ИБ.
3. Политика ИБ компании.
4. Организация ИБ на предприятии.
5. Классификация и управление корпоративными информационными ресурсами.
6. Администрирование безопасности корпоративных информационных систем.
7. Управление доступом.
8. Требования по безопасности к корпоративным информационным системам в ходе их разработки, эксплуатации и сопровождения.
9. Управление бизнес-процессами компании с точки зрения ИБ.
10. Внутренний аудит информационной безопасности компании.

Вторая часть стандарта, определяет возможные функциональные спецификации корпоративных систем управления ИБ с точки зрения их проверки на соответствие требованиям первой части данного стандарта. В соответствии с положениями этого стандарта также регламентируется процедура аудита информационных корпоративных систем.

Главным достоинством данного стандарта является присутствие практических рекомендаций по управлению ИБ.

Главным недостатком данного стандарта, как и у предыдущего, является то, что модель угроз и модель злоумышленника создает разработчик тестируемого программного обеспечения.

Германский стандарт BSI. В отличие от ISO 17799 германское "Руководство по защите информационных технологий для базового уровня защищенности" 1998 посвящено детальному рассмотрению частных вопросов управления ИБ компании. Общая структура германского стандарта BSI приведена на рис. 1.

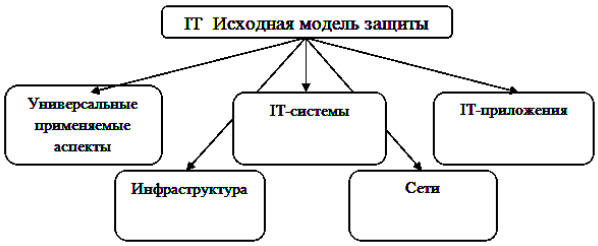

Рис. 1. Структура германского стандарта BSI.

В германском стандарте BSI представлены [5]:

1. Общий метод управления ИБ.
2. Описания компонентов современных информационных технологий.
3. Описания основных компонентов организации режима ИБ.
4. Характеристики объектов информатизации.
5. Характеристики основных информационных активов компании (в том числе аппаратное и программное обеспечение).
6. Характеристики компьютерных сетей на основе различных сетевых технологий, например сети Novell NetWare, сети UNIX и Windows).
7. Характеристика активного и пассивного телекоммуникационного оборудования ведущих вендоров, например Cisco Systems.
8. Подробные каталоги угроз безопасности и мер контроля (более 600 наименований в каждом каталоге).

Основным достоинством стандарта является то, что вопросы защиты оцениваемых информационных активов компании рассматриваются по определенному сценарию: общее описание информационного актива компании (в том числе ОС), возможные угрозы и уязвимости безопасности, предполагаемые меры защиты и средства контроля.

Основным недостатком является сложность оценки влияния угроз на ИБ и эффективности мер защиты ОС.

Сравнительная характеристика стандартов. Описанные в статье стандарты апробированы при разработке систем защиты ОС, имеет свои преимущества и недостатки. В табл. 1 сравниваются наиболее существенные характеристики рассмотренных стандартов.

Как видно из табл. 1 в большинстве стандартов модель злоумышленника составляет производитель

ОС, что существенно уменьшает количество реальных угроз безопасности с которыми сможет справиться оцениваемая ОС. Исключением из этого правила является германский стандарт BSI, в котором эту наиболее важную часть оценки выполняют независимые эксперты.

Таблица 1

Сравнение стандартов безопасности ОС.

	ISO/IEC 15408	**BSI**	**ISO/IEC 17799:2002**
Составление модели злоумышленника	Производитель	Независимые эксперты	Производитель
Составление модели угроз.	Производитель ОС	Производитель ОС	Производитель ОС
Универсальность	-	+	-
Оценка результатов	Производитель	Независимые эксперты	Производитель
Сфера действия	ОС, сетевая инфраструктура.	ОС, компьютер-ные сети, СУБД, прикладное ПО.	ОС, менеджмент ИБ.
Конечный результат использования	Несколько уровней соответствия (для ОС EAL3 – EAL4)	Комплексная оценка ИБ	Несколько уровней соответствия

Модель угроз в каждом рассмотренном стандарте составляется производителем ОС, соответственно даже успешное прохождение сертификации и получение сертификата не гарантирует, что ОС будет защищена от угроз присутствующих при реальной эксплуатации.

Из всех проанализированных стандартов только германский BSI позволяет оценивать безопасность ОС в комплексе с прикладным ПО и сетевой инфраструктурой. Это позволяет более точно оценивать угрозы и риски потери информации или НСД к ней.

Наиболее важно для конечного пользователя это – результат прохождения стандартизации. В стандартах семейства ISO/IEC это – абстрактный уровень защищенности, которому соответствует ОС. Полученный сертификат не всегда гарантирует, что установленная конечная копия ОС будет соответствовать всем заявленным при сертификации параметрам.

При сертификации в германском стандарте BSI пользователь получает пакет документов по сертификации всех компонентов ОС при определенной инфраструктуре предприятия.

Выводы

Использование стандартов безопасности ОС, в которых модель угроз и злоумышленника составляется разработчиком не позволяет в полной мере оценить ИБ. Это объясняется тем, что разработчик для повышения уровня сертификата преднамеренно составляет модель с минимальным, часто не соответствующим реалиям, количеством угроз.

При разработке украинских стандартов безопасности ОС следует использовать типовую модель угроз, учитывающую возможные действия злоумышленников, созданную экспертами в области ИБ. При этом можно отметить, что требования стандартов могут быть усиленны заказчиком при создании ОС.

Список литературы

1. Компьютерная безопасность: вопросы и решения[Электронный ресурс]. – Режим доступа к ресурсу:http://comp-bez.ru/?page_id=2

2. Методические основы защиты информационных активов компании[Электронный ресурс]. http://www.infosecurity.ru/_gazeta/content/031104/article03.html

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

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

5. Шкала рейтингов международных стандартов информационной безопасности [Электронный ресурс] www.cresit-rating.ua/ru/about-rating/scale/12978

Поступила в редколегію 2.04.2012

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

СТАНДАРТИ БЕЗПЕКИ ОПЕРАЦІЙНИХ СИСТЕМ

М.В. Цуранов, О.В. Сліпченко

У статті розглянуті закордонні безпеки операційних систем ISO / IEC 15408, ISO / IEC 17799:2002 (BS 7799:2000) і німецький стандарт BSI, проведена порівняльна оцінка ефективності їх використання.

Ключові слова: *системи міжнародної сертифікації, стандарти безпеки операційних систем, операційна система, модель загроз, модель порушника, ISO / IEC 15408, BSI.э*

SAFETY STANDARDS FOR OPERATING SYSTEMS

M.V. Tsuranov, O.V. Slipchenko

The article deals with foreign operating systems security ISO / IEC 15408, ISO / IEC 17799:2002 (BS 7799:2000) and the German standard of BSI, a comparative assessment of the effectiveness of their use.

Keywords*: system of international certification standards for safety of operating systems, operating system, the threat model, a model offender, ISO / IEC 15408, BSI..*