УДК 004.9

В.А. Корлуженко

КРИТЕРИИ КЛАССИФИКАЦИИ ОБЪЕКТОВ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ

Предлагаются критерии классификации объектов информационных технологий по требованиям безопасности. В результате классификации определяются типовые объекты, для которых целесообразно разрабатывать профили защиты.

Введение

Наиболее распространенным и широко используемым современным стандартом, отражающим набор требований и рекомендаций по обеспечению безопасности продуктов и систем информационных технологий (ИТ), является международный стандарт в области информационной безопасности ИСО/МЭК 15408-99 «Критерии оценки безопасности информационных технологий», больше известный под названием «Общие критерии» (ОК).

Для обеспечения единства понимания излагаемых в статье положений необходимо раскрыть содержание некоторых терминов и понятий ОК [1]. Общие критерии оперируют понятиями «продукты» и «системы ИТ». Под продуктом ИТ понимается отдельное программное, аппаратное или программно-аппаратное средство. Под системой ИТ понимается совокупность средств ИТ, объединенных общими задачами и условиями функционирования. Обобщенным понятием продукта и системы ИТ является объект информационных технологий (ОИТ).

Система и продукт ИТ являются надежными с точки зрения информационной безопасности (ИБ), если удовлетворяют определенным требованиям безопасности. Такие требования представляются в виде специального документа, который принято называть профилем защиты (ПЗ), содержащим функциональные и гарантийные требования безопасности. Так как множество ОИТ велико, международными и национальными стандартами определено, что ПЗ разрабатывается для типового ОИТ. Затем на основе укрупненного ПЗ разрабатывается документ для конкретного ОИТ.

По этим причинам становится актуальной задача классификации ОИТ с целью их объединения в классы по характерным признакам, а также определения типовых объектов, для которых целесообразно разрабатывать ПЗ. Для классификации предложен перечень критериев, учитывающих специфику и разновидности существующих объектов и предназначенных для выделения эквивалентных по определенным признакам классов ОИТ. Таким образом, под критериями подразумеваются признаки, которые используются для принятия решения о принадлежности ОИТ к тому или иному классу. Полученные в результате классификации классы применяются для определения типовых ОИТ.

1. Критерии классификации ОИТ

Для классификации ОИТ предложены следующие критерии [2–4]:

– эквивалентности объектов по степени важности обрабатываемой информации;

– эквивалентности объектов по требуемому уровню защиты;

– эквивалентности объектов по взаимодействию с внешними сетями;

– нахождения в пределах контролируемых зон;

– идентичности используемого состава комплекса средств безопасности объекта (КСБО).

Основой ИБ является обеспечение конфиденциальности, целостности и доступности информации и ресурсов [5]. С учетом этого при классификации ОИТ используется *критерий эквивалентности объектов по степени важности обрабатываемой информации*.

Критерий эквивалентности (подобия) объектов по требуемому уровню защиты применяется для выделения классов ОИТ, требующих различного уровня защиты, так как для достижения необходимого уровня защиты информации и ресурсов формулируются различные тре-

бования безопасности. Существуют три уровня защиты: базовый, расширенный и усиленный. Уровень защиты обеспечивается определенным составом КСБО.

Базовый уровень обеспечивается КСБО, который включает средства безопасности (СБ) операционных систем и антивирусные средства.

Расширенный уровень может обеспечиваться одним из четырех возможных вариантов состава КСБО, который включает СБ:

– базового уровня и межсетевой экран (МЭ);
– базового уровня и обнаружения атак;
– базового уровня и криптографической защиты;
– операционных систем (ОС), обнаружения атак и криптографической защиты.

Усиленный уровень обеспечивается СБ расширенного уровня, дополненными специально разработанными средствами для ОИТ.

Критерий эквивалентности систем по взаимодействию с внешними сетями введен с учетом того, что главными факторами утечки информации являются объединение компьютеров в локальные сети, использующие открытые каналы передачи данных, и наличие подключения к сети Интернет, что порождает ряд проблем ИБ. Применительно к КСБО и продуктам ИТ, участвующим в обработке информации, критерий взаимодействия с внешними сетями не является определяющим.

Критерий нахождения в пределах контролируемых зон введен для выделения ОИТ, в которых существует возможность обеспечения безопасности информации посредством формулировки требований, определяющих физический доступ к объектам и периметр контролируемой зоны.

Критерий идентичности используемого состава КСБО позволяет также выделить классы подобных ОИТ, так как количество наиболее распространенных компонентов КСБО ограничено и невелико. К ним относятся:

– СБ ОС;
– антивирусные средства;
– МЭ;
– средства обнаружения атак;
– средства криптографической защиты;
– специально разработанные СБ для ОИТ с учетом его специфики.

2. Уровни классификации и классы ОИТ

Первый уровень классификации связан с делением ОИТ на системы и продукты ИТ. Соответствующие определения систем и продуктов даны выше. Второй уровень классификации предусматривает различие между системами (продуктами), обрабатывающими информацию, и системами (продуктами), обеспечивающими защиту информации и ресурсов, ввиду того, что к системам (продуктам) различного типа предъявляются различные требования по функциональному назначению и, следовательно, по безопасности.

Для дальнейшей классификации систем (табл. 1 и 2) используются предложенные в п. 1 критерии. В соответствии с табл. 1 система ИТ, обрабатывающая информацию и требующая защиты информации и ресурсов, является типовой, если обрабатывает информацию определенной степени важности, требует определенного уровня защиты, характеризуется определенным взаимодействием с внешними сетями, находится (или не находится) в контролируемой зоне, а также если защита информации и ресурсов обеспечивается определенным составом КСБО.

Типовые системы, обрабатывающие информацию и требующие защиты информации и ресурсов, определяются заданием одного значения для каждого критерия (см. табл. 1). Например, типовой является система, в которой обрабатывается конфиденциальная информация, требуется расширенный уровень защиты информации, не имеется выходов во внешнюю сеть, компоненты находятся в пределах контролируемой зоны, КСБО включает СБ ОС и антивирусные средства.

В соответствии с табл. 2 система ИТ, обеспечивающая защиту информации и ресурсов, является типовой, если защищает информацию определенной степени важности, обеспечивает

определенный уровень защиты, находится (или не находится) в контролируемой зоне. Типовые системы, обеспечивающие защиту информации и ресурсов, определяются заданием одного значения для каждого критерия.

Таблица 1

Критерии классификации и классы систем, обрабатывающих информацию и требующих защиты информации и ресурсов

Критерии	Значения критериев (классы систем)
Эквивалентность систем по степени важности обрабатываемой информации	Классы систем, используемых для обработки информации, которая требует обеспечения: – конфиденциальности; – доступности; – целостности; – конфиденциальности и доступности; – конфиденциальности и целостности; – целостности и доступности; – конфиденциальности, целостности и доступности
Эквивалентность систем по требуемому уровню защиты	Классы систем, требующих: – базового уровня защиты; – расширенного уровня защиты; – усиленного уровня защиты
Эквивалентность систем по взаимодействию с внешними сетями	Классы локальных систем: – не имеющих выхода во внешнюю сеть; – использующих защищенные каналы передачи данных; – использующих открытые каналы передачи данных. Классы распределенных систем, использующих: – защищенные каналы передачи данных; – открытые каналы передачи данных
Нахождение в пределах контролируемых зон	Классы систем: – находящихся в контролируемой зоне; – не находящихся в контролируемой зоне
Идентичность используемого состава КСБО	КСБО включает: – СБ ОС и антивирусные средства; – СБ ОС, антивирусные средства и МЭ; – СБ ОС, антивирусные средства, МЭ и средства обнаружения атак; – СБ ОС, антивирусные средства, МЭ и средства криптографической защиты; – СБ ОС, антивирусные средства, МЭ, средства обнаружения атак и средства криптографической защиты; – СБ ОС, антивирусные средства, МЭ и специально разработанные СБ; – СБ ОС, антивирусные средства, МЭ, средства обнаружения атак и специально разработанные СБ; – СБ ОС, антивирусные средства, МЭ, средства криптографической защиты и специально разработанные СБ; – СБ ОС, антивирусные средства, МЭ, средства обнаружения атак, средства криптографической защиты и специально разработанные СБ

Критерии классификации для продуктов по формулировкам такие же, как и для систем. Отличия касаются взаимодействия с внешними сетями. Применительно к продуктам ИТ критерии взаимодействия с внешними сетями не являются определяющими. В соответствии с таким утверждением можно дать определение типовых продуктов, участвующих в обработке информации, и типовых продуктов-средств защиты.

Продукт ИТ, участвующий в обработке информации, является типовым, если участвует в обработке информации определенной степени важности, требует определенного уровня защи-

ты, находится (или не находится) в контролируемой зоне, а также если защита информации и ресурсов обеспечивается определенным составом КСБО.

Продукт-средство защиты является типовым, если осуществляет защиту информации определенной степени важности, обеспечивает определенный уровень защиты, находится (или не находится) в контролируемой зоне, функционирует в составе определенного КСБО.

Таблица 2

Критерии классификации и классы КСБО*

Критерии	Значения критериев (классы систем)
Эквивалентность КСБО, обеспечивающих защиту информации определенной степени важности	Классы КСБО, предназначенных для защиты информации, которая требует обеспечения: – конфиденциальности; – доступности; – конфиденциальности и доступности; – конфиденциальности и целостности; – целостности и доступности; – конфиденциальности, целостности и доступности
Эквивалентность КСБО, обеспечивающих определенный уровень защиты информации	Классы КСБО, обеспечивающих: – базовый уровень защиты; – расширенный уровень защиты; – усиленный уровень защиты
Нахождение КСБО в пределах контролируемых зон	Классы КСБО: – находящихся в контролируемой зоне; – не находящихся в контролируемой зоне

*Понятия «система, обеспечивающая защиту информации и ресурсов» и «КСБО» идентичны

3. Формализованное представление типовых ОИТ

На основании вышеизложенного (см. табл. 1) для формализованного представления типовых систем, обрабатывающих информацию и требующих защиты информации и ресурсов, введем пять множеств классов систем, различающихся по следующим признакам [6]:

– степени важности обрабатываемой информации, $E = \{e_b\}$, $b = \overline{1,B}$, где B – количество значений данного критерия, $B = 7$;

– требуемому уровню защиты, $U = \{u_m\}$, $m = \overline{1,M}$, где M – количество значений данного критерия, $M = 3$;

– взаимодействию с внешними сетями, $S = \{s_n\}$, $n = \overline{1,N}$, где N – количество значений данного критерия, $N = 5$;

– нахождению в пределах контролируемой зоны, $Z = \{z_k\}$, $k = \overline{1,K}$, где K – количество значений данного критерия, $K = 2$;

– используемому составу КСБО, $H = \{h_l\}$, $l = \overline{1,L}$, где L – количество значений данного критерия, $L = 9$.

Множество T типовых систем, обрабатывающих информацию и требующих защиты информации и ресурсов, является подмножеством декартова произведения ранее введенных множеств:

$$T \subset E \times U \times S \times Z \times H = \{t_\psi =< e_b, u_m, s_n, z_k, h_l >\},\ \psi = B \cdot M \cdot N \cdot K \cdot L = 1890,$$

$$b = \overline{1,7},\ m = \overline{1,3},\ n = \overline{1,5},\ k = \overline{1,2},\ l = \overline{1,9}.$$

Множество T типовых систем является именно подмножеством декартова произведения множеств $E \times U \times S \times Z \times H$ ввиду того, что некоторые комбинации $(e_b, u_m, s_n, z_k, h_l)$ не образуют типовую систему $t_\psi =< e_b, u_m, s_n, z_k, h_l >$, т. е. выполняется условие

$$\exists(e_b)\exists(u_m)\exists(s_n)\exists(z_k)\exists(h_l):\ \exists(t_\psi =< e_b, u_m, s_n, z_k, h_l >) \notin T,$$

так как типовых систем некоторых комбинаций в соответствии с предложенными критериями не существует. Например, конфиденциальная информация не может обрабатываться в системе, использующей открытые каналы передачи данных и т. д.

Аналогичным образом в соответствии с табл. 2 описывается множество типовых КСБО. Множество T' типовых КСБО является подмножеством декартова произведения множеств E', U', Z':

$$T' \subset E' \times U' \times Z' = \{t'_\gamma =< e'_b, u'_m, z'_k >\},\ \Gamma = B \cdot M \cdot K = 42,\ b = \overline{1,7},\ m = \overline{1,3},\ k = \overline{1,2}.$$

Аналогично описываются и множества типовых продуктов. Множество T_p типовых продуктов, участвующих в обработке информации, является подмножеством декартова произведения множеств E_p, U_p, Z_p, H_p:

$$T_p \subset E_p \times U_p \times Z_p \times H_p = \{t_{p_\lambda} =< e_{p_b}, u_{p_m}, z_{p_k}, h_{p_l} >\},\ \Lambda = B \cdot M \cdot K \cdot L = 378,$$
$$b = \overline{1,7},\ m = \overline{1,3},\ k = \overline{1,2},\ l = \overline{1,9}.$$

Множество T'_p типовых продуктов-средств защиты информации и ресурсов является подмножеством декартова произведения множеств E'_p, U'_p, Z'_p, H'_p:

$$T'_p \subset E'_p \times U'_p \times Z'_p \times H'_p = \{t'_{p_\chi} =< e'_{p_b}, u'_{p_m}, z'_{p_k}, h'_{p_l} >\},\ \mathrm{X} = B \cdot M \cdot K \cdot L = 378,$$
$$b = \overline{1,7},\ m = \overline{1,3},\ k = \overline{1,2},\ l = \overline{1,9}.$$

Заключение

В соответствии с предложенными критериями многочисленное множество объектов представляется множествами типовых ОИТ. Множества типовых систем и продуктов задаются различными сочетаниями соответствующих классов. Однако некоторые сочетания на практике не существуют, вследствие чего потребность в разработке ПЗ для них отсутствует. На основании установленных критериев типовому ОИТ можно поставить в соответствие ряд характеристик, которыми должен обладать его ПЗ. Эти сведения могут быть использованы разработчиками при проектировании и экспертами при оценке ПЗ.

Список литературы

1. Фисенко, В.К. Критерии классификации объектов информационных технологий по требованиям информационной безопасности / В.К. Фисенко, Е.П. Максимович // Материалы IX Междунар. конф. «Комплексная защита информации», 1–3 марта 2005 г., Раубичи, Беларусь. – Минск: ОИПИ НАН Беларуси, 2005. – С. 103–105.

2. О некоторых подходах к категорированию объектов информатизации по требованиям информационной безопасности / В.В. Анищенко [и др.] // Сб. науч. тр. «Комплексная защита информации». Вып. 3. – Минск: Ин-т техн. кибернетики НАН Беларуси, 2000. – С. 5–22.

3. Методика категорирования автоматизированных систем по уровню защищенности информации от несанкционированного доступа / Ю.Г. Кирсанов [и др.] // Вопросы защиты информации. – 1997. – № 3, 4. – С. 36–39.

4. СТБ 34.101.1 – 2004. Информационные технологии и безопасность. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. – Введен 01.02.2005 г.

5. Зегжда, Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. – М.: Горячая линия – Телеком, 2000.

6. Калужнин, Л.А. Что такое математическая логика? / Л.А. Калужнин. – М.: Наука, 1964.

Поступила 27.10.06

Объединенный институт проблем
информатики НАН Беларуси,
Минск, Сурганова, 6
e-mail: fisenko@newman.bas-net.by

V.A. Korluzhenko

THE CLASSIFICATION CRITERIA OF INFORMATION TECHNOLOGY OBJECTS BY SECURITY REQUIREMENTS

The classification criteria of information technology objects by security requirements are considered. As the result of the classification the typical objects of the information technologies for which it is necessary to develop protection profiles are defined.