Оценка киберрисков на множестве параметров безопасности ОС Windows XP/2003

Р. А. Абдульманов, М. О. Калинин

Согласно ГОСТ Р ИСО 17799 под оценкой киберрисков понимается систематический анализ вероятного ущерба, наносимого в результате нарушений в сфере информационной безопасности с учетом последствий от потери конфиденциальности, целостности или доступности информации [1].

В современных методиках и реализованных на их основе программных средствах, применяемых для оценки рисков, информационная система рассматривается с обобщенных позиций. Посредством анкетирования эксперты описывают информационные активы и ресурсы систем, учитывая количественные и стоимостные характеристики, взаимосвязи компонентов, вероятные уязвимости безопасности. Примерами таких методов являются CRAMM [2], ISO/IEC 17799:2005, Marion.

Однако при оценке рисков информационной безопасности в современных системах высокоуровневое описание компонентов (рис. 1) является недостаточным, т. к. оно не учитывает наличие сложной распределенной архитектуры, неявных взаимосвязей активов и информационных ресурсов, механизмов управления информационными потоками, особенностей организации подсистем контроля и управления доступом. На рис. 2 представлено влияние влияние системных параметров безопасности и их взаимосвязей на организацию доступа к ресурсам информационной системы.

Таким образом, оценивая риск нарушения безопасности системы, построенной на базе ОС Windows, эксперт должен учитывать такие параметры безопасности, как иерархия файловой системы, структура системного реестра, распространение прав доступа, назначаемых субъектам, привилегии пользователей и т. п.

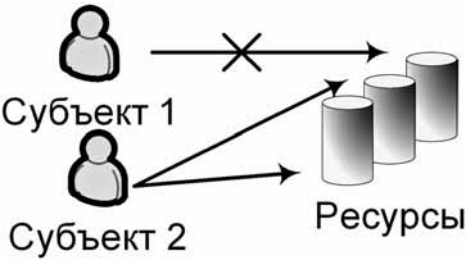

Рис. 1. Пример высокоуровневого представления информационного взаимодействия при оценке рисков

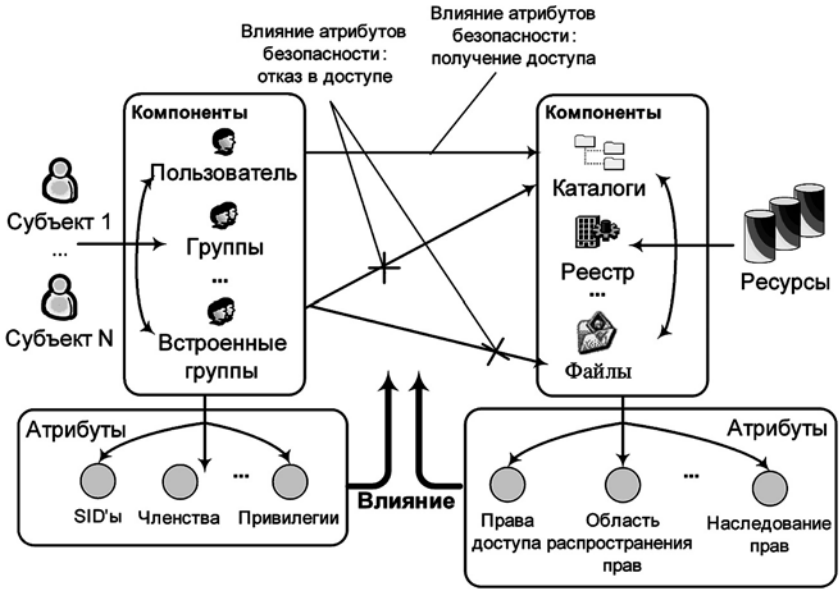

Рис 2. Пример низкоуровневого представления информационного взаимодействия при оценке рисков

С одной стороны, количество параметров безопасности, участвующих в организации контроля и управления доступом, а также их взаимосвязей, огромно и не может быть подвергнуто оценке, выполняемой экспертом с использованием традиционного подхода на основе анкетирования. С дру-

гой стороны, не учитывать при оценке рисков информационной безопасности множество этих параметров нельзя, т. к. они могут послужить причиной недопустимого получения доступа непривилегированными пользователями к секретной информации организации или недоступности информационных ресурсов. Следовательно, при оценке информационных рисков в системах, в которых контроль и управление доступом осуществляется посредством управления параметрами безопасности, требуется разработка нового подхода к оценке киберрисков, позволяющего учитывать эти особенности организации защиты.

Авторами предложен подход, позволяющий проводить оценку риска уязвимости систем на множестве параметров безопасности ОС Windows XP/2003, по результатам которой возможно определить множество объектов ОС, оказавших наибольшее влияние на увеличение риска нарушения безопасности.

Рассмотрим систему как совокупность компонентов, ее составляющих. Будем называть компонентом объединение множеств объектов системы и их параметров безопасности. Множество объектов составляют следующие участники безопасности [3–5]:

- локальные и доменные пользователи и группы пользователей;
- объекты файловой системы NTFS;
- объекты системного реестра.

Примером компонента является браузер *Internet Explorer*, который на системном уровне представляется как множество объектов файловой системы в папке *%ProgramFiles%\Internet Explorer* и ключей реестра в разделе *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer*

Для определения влияния разных компонентов на организацию безопасности системы применяются весовые коэффициенты. При этом множество весов разделяется на два набора: весовые коэффициенты, выбираемые экспертами для определения значимости оцениваемых информационных ресурсов с точки зрения безопасности, и уточняющие весовые коэффициенты, автоматически вычисляемые в ходе оценки с целью корректировки первого набора коэффициентов. Экспертами создается своего рода эталон — база объектов и их параметров безопасности, а также с ними сопоставленные весовые коэффициенты. Эталонные значения сравниваются с текущими параметрами безопасности системы, и на основании такого сравнения вычисляются уточняющие коэффициенты. Уточняющие коэффициенты позволяют скорректировать эталонную базу и произвести более точную оценку с учетом параметров безопасности каждого объекта, входящего в компонент в системе.

Оцениваемая система разбивается на множество ее составляющих компонентов. Коэффициент значимости для безопасности *i*-го компонента, влияющего на оценку рисков, рассчитывается по формуле:

$$Ko_i = \frac{Kp_i}{Kp_{\max}} \cdot Kf_i,$$

где Kp_i — коэффициент значимости, задаваемый экспертом,

$Kp_{\max}$ — максимальное значение коэффициента Kp_i,

Kf_i — уточняющий коэффициент, рассчитанный на основании параметров безопасности объектов, входящих в состав компонента.

Уточняющий коэффициент рассчитывается по формуле:

$$Kf_i = \left(1 - \frac{n}{\sum_{j=1}^{n} (Kc_{i,j} + Kext) \cdot Ku}\right),$$

где n — количество объектов, входящих в состав одного *i*-го компонента,

$Kc_{i,j}$ — коэффициент значимости *j*-го объекта, входящего в *i*-й компонент,

$Kext$ — коэффициент значимости типа объекта, который показывает увеличение влияния для наиболее значимых объектов (например, исполняемых файлов, драйверов) и уменьшение — для наименее значимых (например, рисунков, временных файлов).

Ku — коэффициент значимости прав доступа субъектов к *j*-ому объекту.

Коэффициент значимости прав доступа для каждого объекта рассчитывается по формуле:

$$Ku = \frac{m \cdot \sum_{h=1}^{m} \left(Ku_h \cdot \sum_{l=1}^{p} (Kpr_l) \right)}{k},$$

где m — количество прав доступа, отличающихся от эталонных,

k — общее количество прав, заданных относительно данного объекта,

Ku_h — коэффициент значимости субъекта или группы, заданный экспертом,

Kpr — коэффициент значимости привилегии (в случае ее наличия у субъекта). Учет значимости привилегий отражает возможность получения прав доступа субъектом.

p — общее количество учитываемых привилегий.

Если интерпретировать нарушения конфиденциальности как несоответствия между эталонным распределением прав на чтение объектов и фактическим, целостности — прав на запись, доступности — прав на выполнение, то общая оценка риска системы представляет собой три оценки рисков нарушения конфиденциальности, целостности и доступности, соответственно. Каждая из оценок рассчитывается независимо по формуле:

$$R = 1 - \prod_{i=1}^{n} (1 - Ko_i),$$

где n — количество анализируемых компонентов системы.

Если известна общая стоимость информационного ресурса, финансовый риск оценивается по формуле:

$$Rm = R \cdot M,$$

где R — риск связанный с нарушением конфиденциальности, целостности или доступности,

M — стоимость информационного ресурса.

В качестве примера использования предложенного подхода рассмотрим пример оценки рисков для компонента ОС Windows *Internet Explorer* (IE).

Признаком присутствия компонента в системе является наличие объекта-каталога *%ProgramFiles%\Internet Explorer*. Ввиду использования браузера IE большим числом пользователей, а также его интегрированности в систему, базовый коэффициент значимости этого компонента устанавливается экспертом, например, равным 8 (из диапазона 0 … 10).

Согласно настройкам после установки ОС Windows атрибуты безопасности объектов компонента IE можно описать следующим образом (рис. 3). Пример задания коэффициентов типов объектов (из диапазона —10 … + 10)

представлен на рис. 4. Пример задания коэффициентов значимости привилегий (из диапазона 1 … 10) приведен на рис. 5. Пример задания коэффициентов значимости субъектов (из диапазона 0 … 10) представлен на рис. 6.

Допустим в системе разрешен доступ на запись и чтение пользователю *TestUsr*, включенного в группу *Пользователи*, к каталогу с установленным компонентом IE, а также полный доступ к исполняемому файлу *IEXPLORE.EXE*.

Объект	Коэфф.	Распространение прав (каталог/подкаталог/файл)			Наследование	Привилегированные пользователи	Опытные пользователи	Пользователи
%ProgramFiles%\Internet Explorer*	8	+	+	+	да	F	RWX	RX
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Internet Explorer*	6	+	+		да	F	RWX	RX

F - полный доступ R - чтение W - запись X - исполнение

Рис. 3. Параметры безопасности и коэффициенты значимости объектов компонента IE

Тип	Коэфф.
.	0
*.txt	-10
*.exe	9
*.dll	7

Рис. 4. Таблица коэффициентов значимости типов объектов

Название	Коэфф.
Восстановление файлов и каталогов	5
Овладение файлами или иными объектами	7

Рис. 5. Таблица коэффициентов значимости привилегий

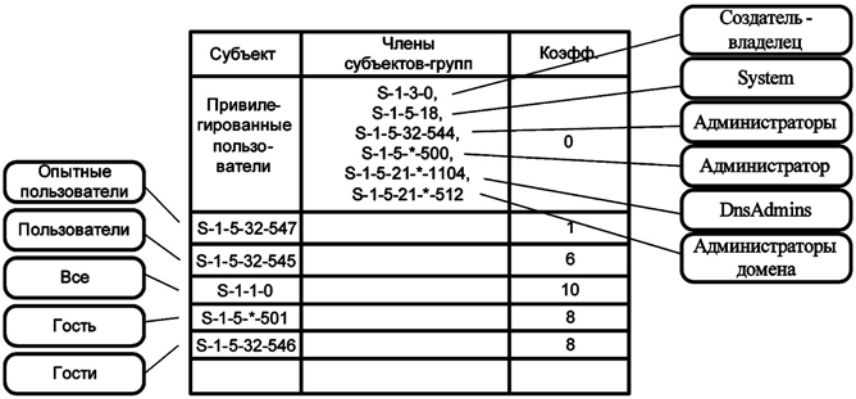

Рис. 6. Таблица коэффициентов значимости субъектов

Согласно этим текущим параметрам безопасности и ранее заданным эталонным таблицам (рис. 3 … 6), расчет итоговых рисков производится следующим образом:

Для нарушения конфиденциальности: $R = 0$ — риски, связанные с нарушением конфиденциальности, отсутствует. Пользователь *TestUsr* является членом группы *Пользователи*, а ей соответствующий доступ на чтение разрешен.

Для нарушения целостности:

$$Kf_1 = \left(1 - \frac{33}{((8+0)+(8+9)) \cdot K_u}\right), \quad K_u = \frac{2(6 \cdot 7 + 6 \cdot 7)}{6} = 28,$$

$$Kf_1 = 0,95, \quad Ko_1 = \frac{8}{10}\ 0,95 = 0,76, \quad R = 1 - (1 - 0,76) = 0,76.$$

Риски, связанные с нарушением целостности, высокие. Пользователь *TestUsr* имеет право на модификацию каталога IE, не определенное в исходной таблице, а также исполняемого файла *IEXPLORE.EXE*. Следовательно, этот пользователь может их изменить, поставив тем самым под угрозу функционирование системы в целом. Примером такого изменения является добавление вредоносного кода.

Для нарушения доступности: $R = 0$ — риски, связанные с нарушением доступности, отсутствуют. Пользователь *TestUsr* не имеет права вы-

полнения на каталог IE, но группа *Пользователи*, к которой он принадлежит, такое право имеет.

Таким образом, в статье рассмотрен математический подход, позволяющий произвести оценку киберрисков уязвимости информационных систем на множестве параметров безопасности. Данный подход может быть автоматизирован и по результатам оценки могут предприниматься активные действия направленные на уменьшение риска путем внесения изменений в настройки безопасности.

Литература

1. Федеральное агентство по техническому регулированию и метрологии, ГОСТ Р ИСО/МЭК 17799-2005. С. 5.
2. *Симонов С. В.* Анализ рисков, управление рисками. М.: Jet Info. 1999. № 1. С. 11–17.
3. Ресурсы Microsoft Windows NT Server 4.0. Книга 1. СПб.: БХВ-Петербург, 2001. 408 С.
4. *Schultz E. E.* Windows NT/2000 Network Security. Macmillan Technical Publishing, 2000. 437 P.
5. *Брагг Р.* Система безопасности Windows 2000. М.: Изд. дом «Вильямс», 2001. 592 С.