УДК 004.056.5

В.Г. Миронова, Н.Т. Югов, А.А. Мицель

Методология проведения анализа режимов разграничения прав доступов пользователей к конфиденциальной информации и возможности осуществления несанкционированного доступа

Представлена методология проведения анализа режимов разграничения прав доступов пользователей к конфиденциальной информации и возможности осуществления несанкционированного доступа. В основе методологии лежит дискреционная модель разграничения прав доступа к информации модели Take-Grant.

Ключевые слова: разграничение прав, Take-Grant, конфиденциальная информация, несанкционированный доступ.

Основой любой системы защиты информации (СЗИ) является подсистема контроля и управления доступом, которая включает в себя процедуры идентификации и аутентификации. Эти процедуры защиты информации рассчитаны на работу с субъектами и объектами информационной системы (ИС) поименно. Определения этих понятий четко сформулированы в [1, 2].

Напомним, что в качестве субъектов ИС могут выступать как пользователи, так и процессы, а в качестве объектов ИС – информация и другие информационные ресурсы системы. Безусловно, при создании системы защиты проводится анализ существующих субъектов и объектов в ИС. Основные этапы построения СЗИ подробно описаны в [3].

Одним из этапов создания СЗИ является построение моделей нарушителя и угроз безопасности конфиденциальной информации (КИ). Порядок построения модели нарушителя безопасности изложен в [4], а подходы к проведению анализа угроз безопасности КИ – в [5–7].

На этапе построения модели нарушителя ИБ важно не только определить отличительные черты нарушителей – субъектов ИС, но и выявить возможные сговоры и случаи возможного предоставления доступа к КИ.

При проведении анализа режимов разграничения и распространения прав доступа аутентифицированных субъектов важно руководствоваться политикой ИБ. В [8] представлено описание существующих подходов к реализации политики ИБ. В настоящее время популярной является дискреционная политика ИБ (ДПИБ). Для проведения анализа режимов разграничения и распространения прав доступа при реализации ДПИБ была выбрана модель распространения прав доступа Take-Grant.

Формально описание модели Take-Grant выглядит следующим образом:

1. Множество объектов – **O**, где $o_j \in \mathbf{O}$, $\mathbf{O} = \{o_1, o_2, \ldots, o_j\}$, $j \in \mathbf{N}$;

2. Множество субъектов – **S**, где $s_n \in \mathbf{S}$, $\mathbf{S} = \{s_1, s_2, \ldots, s_n\}$, $n \in \mathbf{N}$;

3. Множество прав доступа **R**, где $r_i \in \mathbf{R}$, $\mathbf{R} = \{r_1, r_2, \ldots, r_j\} \cup \{t, g\}$, где t (take) – право брать права доступа, g (grant) – права давать права доступа.

G = (**S**, **O**, **E**) – конечный помеченный ориентированный без петель граф доступов, описывающий состояние системы. При этом вершинами графа **G** являются элементы **S** и **O**. Каждое ребро графа **G** имеет метку из множества видов прав доступа **R**.

Порядок перехода системы из состояния в состояние определяется правилами преобразования графа доступов, которые в классической модели носят название де-юре правил. Возможность передачи прав между двумя удаленными субъектами определяется с помощью предиката «Возможен доступ» (β, x, y, **G**), который будет истинным тогда и только тогда, когда существует цепочка преобразований графа **G** с помощью правил де-юре, в результате которых появляется дуга от объекта x к объекту y с правом β [8].

Граф доступов **G** = (**S**, **S**, **E**), все вершины которого представлены субъектами, является tg-связным или соединен tg-путем, когда без учета направления ребер в графе между ними существует путь такой, что каждое ребро этого пути помечено t или g.

Основным подходом к определению вероятности возникновения НСД в ИС является присваивание веса (стоимости) каждому ребру графа. Тогда возможность осуществления НСД будет складываться из суммы весов дуг доступов по соответствующим ребрам.

Обозначим множество вершин tg-графа $\mathbf{G_{tg}}$ через **V**, а множество дуг через **D**. Построим для выявления tg-путей новый не помеченный и не ориентированный граф $\mathbf{G_{tg}}$ на основе графа **G** по следующим правилам:

1) множество вершин графа $\mathbf{G_{tg}}$ совпадает с множеством вершин графа **G**;

2) если метка дуги в графе **G** включает в себя **t** или **g**, то добавляем в графе $\mathbf{G_{tg}}$ дугу между соответствующими вершинами. Граф $\mathbf{G_{tg}}$ характеризует связь вершин с помощью tg-путей.

В графе $\mathbf{G_{tg}}$ отношение инцидентности будем задавать с помощью матрицы смежности **E**. Матрицей смежности графа $\mathbf{G_{tg}}$ в этом случае является матрица **E** размерностью $n \times n$, (где n – число вершин графа), однозначно представляющая его структуру. А именно, если существует дуга из вершины v_i в вершину v_j, то существующий элемент матрицы смещения $\mathbf{E}_{ij} = 1$, в противном случае $\mathbf{E}_{ij} = 0$, также будем полагать, что в графе нет петель, и полагать $\mathbf{E}_{ij} = 0$. Поскольку граф $\mathbf{G_{tg}}$ будет рассматриваться как граф без петель, то в матрице смежности $\mathbf{G_{tg}}$ по главной диагонали будут стоять нулевые элементы.

Если **E** – матрица смежности графа $\mathbf{G_{tg}}$, то в графе существует маршрут между вершинами v_i и v_j тогда и только тогда, когда (i, j)-й элемент матрицы $\mathbf{E} + \mathbf{E}^2 + \ldots + \mathbf{E}^{n-1}$ не равен нулю.

Алгоритм поиска возможных путей доступа между субъектами:

1. Выделить количество участвующих субъектов.
2. Построить граф доступов **G**.
3. Построить матрицу доступов графа **G**.
4. Построить граф $\mathbf{G_{tg}}$.
5. Построить матрицу смежности **E**.
6. Определить веса дуг, построить матрицу меток дуг.
7. Определить маршруты по матрице смежности.
8. Определить стоимости полученных маршрутов.

Рассмотрим несколько типов графов доступов для разного количества участвующих субъектов. Пусть количество субъектов – 3.

1. Количество участвующих субъектов – s_1, s_2, s_3.
2. Граф доступов **G** (рис. 1).

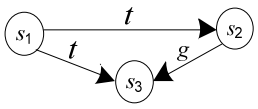


Рис. 1. Граф доступов **G**

3. Матрица доступов графа **G** (табл. 1).

Таблица 1

Матрица доступов графа G

	s_1	s_2	s_3
s_1	F	t	
s_2		F	
s_3	t	g	F

4. Построить граф $\mathbf{G_{tg}}$ (рис. 2).

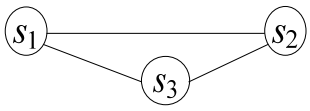


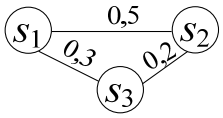
Рис. 2. Граф $\mathbf{G_{tg}}$

5. Построить матрицу смежности **E** (рис. 3).

$$\mathbf{E} = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

Рис. 3. Матрица смежности **E**

6. Веса дуг, матрица меток дуг (рис. 4).



$$\mathbf{E}=\begin{pmatrix} 0 & 0{,}5 & 0{,}3 \\ 0{,}5 & 0 & 0{,}2 \\ 0{,}3 & 0{,}2 & 0 \end{pmatrix}.$$

Рис. 4. Веса дуг, матрица меток дуг

7. Маршруты по матрице смежности. Максимальная длина маршрута $l = 3$ (рис. 5):
при длине пути 1

$$\mathbf{E}=\begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix};$$

при длине пути 2

$$\mathbf{E}=\begin{pmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{pmatrix}.$$

Рис. 5. Маршруты по матрице смежности

8. Стоимость полученных маршрутов (рис. 6):
при длине пути 1

$$\mathbf{S}=\begin{pmatrix} 0 & 0{,}5 & 0{,}3 \\ 0{,}5 & 0 & 0{,}2 \\ 0{,}3 & 0{,}2 & 0 \end{pmatrix};$$

при длине пути 2

$$\mathbf{S}=\begin{pmatrix} 0 & 0{,}5 & 0{,}7 \\ 0{,}5 & 0 & 0{,}8 \\ 0{,}7 & 0{,}8 & 0 \end{pmatrix}.$$

Рис. 6. Стоимость полученных маршрутов

Пусть количество субъектов равно 4, тогда:
1. Количество участвующих субъектов – s_1, s_2, s_3, s_4.
2. Граф доступов **G** (рис. 7).

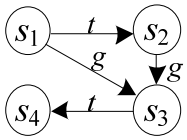


Рис. 7. Граф доступов **G**

3. Матрица доступов графа **G** (табл. 2).

Таблица 2

Матрица доступов графа G

	s_1	s_2	s_3	s_4
s_1	F	t	g	
s_2		F	g	
s_3			F	t
s_4				F

4. Построить граф $\mathbf{G_{tg}}$ (рис. 8).

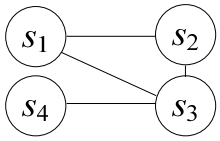


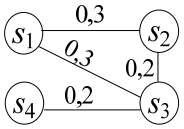
Рис. 8. Граф $\mathbf{G_{tg}}$

5. Построить матрицу смежности **E** (рис. 9).

$$\mathbf{E}=\begin{pmatrix}0&1&1&0\\1&0&1&0\\1&1&0&1\\0&0&1&0\end{pmatrix}.$$

Рис. 9. Матрица смежности **E**

6. Веса дуг, матрица меток дуг (рис. 10).



$$\mathbf{E}=\begin{pmatrix}0&0{,}3&0{,}3&0\\0{,}3&0&0{,}2&0\\0{,}3&0{,}2&0&0{,}2\\0&0&0{,}2&0\end{pmatrix}.$$

Рис. 10. Веса дуг, матрица меток дуг

7. Маршруты по матрице смежности. Максимальная длина маршрута $l = 3$ (рис. 11).

$$\mathbf{E}=\begin{pmatrix}0&1&1&0\\1&0&1&0\\1&1&0&1\\0&0&1&0\end{pmatrix}.$$

$$\mathbf{E}=\begin{pmatrix}2&1&1&1\\1&2&1&1\\1&1&3&1\\1&1&0&1\end{pmatrix}.$$

Рис. 11. Маршруты по матрице смежности

8. Стоимость полученных маршрутов (рис. 12):
при длине пути, равном 1

$$\mathbf{S}=\begin{pmatrix}0&0{,}3&0{,}3&0\\0{,}3&0&0{,}2&0\\0{,}3&0{,}2&0&0{,}2\\0&0&0{,}2&0\end{pmatrix};$$

при длине пути, равном 2

$$\mathbf{E}=\begin{pmatrix}0&0{,}5&0{,}5&0\\0{,}5&0&0{,}6&0\\0{,}5&0{,}6&0&0\\0&0&0&0\end{pmatrix};$$

при длине пути, равном 3

$$\mathbf{E}=\begin{pmatrix}0&0&0&0{,}7\\0&0&0&0{,}8\\0&0&0&1\\0{,}7&0{,}8&0&0\end{pmatrix}.$$

Рис. 12. Стоимость полученных маршрутов

Выявляя вероятностных нарушителей ИБ, важно не только знать их отличительные особенности, но и выявлять и оценивать возможные пути получения доступа к КИ нарушителем, проводить анализ путей распространения прав доступа.

С помощью предложенного подхода с использованием правил модели Take-Grant можно оценить возможные пути распространения прав доступа к КИ по длине и провести анализ их стоимости. Такой подход позволяет быстро и оперативно выявлять взаимодействия пользователей ИС с нарушителями ИБ, давать оценку таким взаимодействиям, формировать способы нейтрализации таких взаимодействий.

Литература

1. Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам / под ред. А.А. Шелупанова, С.Л. Груздева, Ю.С. Нахаева. – М.: Горячая линия – Телеком, 2009. – 552 с.

2. Мещеряков Р.В. Комплексное обеспечение информационной безопасности автоматизированных систем / Р.В. Мещеряков, А.А. Шелупанов. – Томск: В-Спектр, 2007. – 278 с.

3. Автоматизированная система предпроектного обследования информационной системы персональных данных «АИСТ-П» / А.А. Шелупанов, В.Г. Миронова, С.С. Ерохин, А.А. Мицель // Доклады ТУСУРа. – 2010. – № 1 (21), ч. 1. – С. 14–22.

4. Миронова В.Г. Модель нарушителя безопасности конфиденциальной информации / В.Г. Миронова, А.А. Шелупанов // Информатика и системы управления. – 2012. – № 1 (31). – С. 28–35.

5. Прищеп С.В. Подходы и критерии оценки рисков информационной безопасности / С.В. Прищеп, С.В. Тимченко, А.А. Шелупанов // Безопасность информационных технологий. – 2007. – № 4. – С. 15–21.

6. Технология прямого поиска при решении задач прикладной математики / В.А. Архипов, С.С. Бондарчук, И.Г. Боровской, А.А. Шелупанов // Вычислительные технологии. – 1995. – Т. 4, № 10. – С. 19.

7. Миронова В.Г. Методология формирования угроз безопасности конфиденциальной информации в неопределенных условиях их возникновения / В.Г. Миронова, А.А. Шелупанов // Известия Южного федерального университета. Технические науки. – 2012. – Т. 137, № 12. – С. 39–45.

8. Миронова В.Г. Реализация модели Take-Grant как представление систем разграничения прав доступа в помещениях / В.Г. Миронова, А.А. Шелупанов, Т.Н. Югов // Доклады ТУСУРа. – 2011. – № 2 (24), ч. 3. – С. 206–211.

9. Криптографические протоколы в системах с ограниченными ресурсами / Р.В. Мещеряков, С.К. Росошек, А.А. Шелупанов, М.А. Сонькин // Вычислительные технологии. – 2007. – Т. 12, Спецвыпуск №1. – С. 51–61.

10. Встраивание криптографических функций в систему связи с ограниченными ресурсами / С.К. Росошек, Р.В. Мещеряков, А.А. Шелупанов, С.С. Бондарчук // Вопросы защиты информации. – 2004. – № 2. – С. 22–25.

Миронова Валентина Григорьевна
Канд. техн. наук, мл. науч. сотр. каф. комплексной информационной безопасности электронно-вычислительных систем ТУСУРа
Тел.: +7-923-415-16-08
Эл. почта: mvg@security.tomsk.ru

Югов Николай Тихонович
Д-р физ.-мат. наук, профессор каф. математики ТУСУРа
Эл. почта: office@keva.tusur.ru

Мицель Артур Александрович
Д-р техн. наук, профессор каф. автоматизированных систем управления ТУСУРа
Тел.: +7 (382-2) 70-15-36
Эл. почта: maa@asu.tusur.ru

Mironova V.G., Ugov N.T., Mitsel A.A.

The methodology for the analysis of modes of differentiation of user access rights to confidential information and the possibility of unauthorized access

The article presents a methodology for the analysis of modes of differentiation of user access rights to confidential information and the possibility of unauthorized access . The methodology is discretionary model differentiation of access rights to information model Take-Grant.
Keywords: divestiture, Take-Grant, confidential information, unauthorized access.