2008 Математические основы компьютерной безопасности № 1(1)

DOI 10.17223/20710410/1/13
УДК 004.56(06)

СОВРЕМЕННЫЕ МОДЕЛИ И МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ

М.М. Кучеров, И.Н. Кирко, А.А. Муллер

Сибирский федеральный университет, *г. Красноярск*

E-mail: kucherov@fivt.krgtu.ru

Разработана решеточная модель информационной безопасности, суть которой состоит в использовании общего уровня для целостности и доступности. Уровни, характеризующие целостность и доступность, совместно указывают на объективное качество в модели ценности информации.

***Ключевые слова*:** *мандатный контроль и управление доступом*, *закон Гроша*, *эффективность доступа.*

Сегодня многие организации объединяют ресурсы. Такое объединение выгодно всем участникам информационного обмена. При объединении фирм также происходит объединение общих электронных документов, файлов, баз данных и т.д. Для того чтобы обеспечить безопасность информации, необходим процесс управления информацией и разграничение доступа внутри и за пределами каждой организации.

Управление информацией предполагает, что известен объем информации, требуемый для управления производством. Невозможно, фактически, подробно перечислить информационные объекты, но можно назвать основные элементы информации, необходимые для производственных операций. Элемент информации представляет собой основную часть информации. Он может появляться в разных местах в ментальной, письменной или электронной форме.

Основной элемент информации имеет следующие свойства:

- является существенным для производства;
- создается первичной производственной функцией;
- может находиться в разнообразных сочетаниях с другой информацией.

Список основных элементов информации, существенных для производства, указывает на элементы информации, которые являются объектами управления и контроля. Решение о том, будет или не будет предприятие контролировать соответствующий элемент информации, зависит от его значения. В случае создания новых элементов информации или использования уже существующих элементов руководство предприятием должно предпринять необходимые действия для того, чтобы эти элементы информации имели соответствующее значение, что позволило бы при необходимости контролировать их надлежащим образом.

Запросы на информацию постоянно возрастают с увеличением объемов производства. Закон Гроша утверждает, что увеличение в n раз отдачи от инвестиций в компьютерное оборудование возможно при увеличении в n^2 раз скорости обработки информации, т.е. сокращении в соответствующее число раз времени доступа к информации [1, 8]. Почти невозможно предвидеть требования на доступ к центральным базам данных, а также приложения, с помощью которых будет обработана полученная информация. Следовательно, важно, чтобы элементы информации были отделены от производственных приложений и находились в форме, позволяющей легко их использовать для разных приложений и целей.

1. Определения

Вначале дадим необходимые определения [2 – 6]. Мандатное управление доступом есть разграничение доступа субъектов к объектам, основанное на характеризуемой меткой конфиденциальности информации, содержащейся в объектах и официальном разрешении (допуске) субъектов обращаться к информации такого уровня конфиденциальности.

Под уровнем конфиденциальности будем понимать иерархический атрибут, который может быть ассоциирован с сущностью компьютерной системы для обозначения степени ее критичности в смысле безопасности. Этот атрибут может обозначать, например, степень ущерба от нарушения безопасности в компьютерной системе или чувствительность (чувствительность — характеристика ресурса, которая определяет его ценность или важность и может учитывать его уязвимость).

Степень доверия — это атрибут, определяющий уровень конфиденциальности субъекта. Чем выше степень доверия субъекта, тем к более секретной информации он имеет доступ. Чем выше конфиденциальность объекта, тем более секретная информация хранится в нем.

Определим функции, отображающие субъектов и объекты системы, на уровни конфиденциальности — допуск (*clearance*) и гриф (*classification*). Областью значений каждой из этих функций является решетка уровней конфиденциальности L с линейным отношением частичного порядка. Функция *clearance* определе-

на на множестве субъектов *S*, а *classification* — на множестве объектов *O*. Эти функции записываются следующим образом:

$$clearance\ (s) = l_s; \tag{1}$$

$$classification\ (o) = l_o. \tag{2}$$

Кроме уровней конфиденциальности, можно ввести множество категорий. Каждая категория описывает соответствующий тип информации. Примерами категорий могут служить {«Для прессы», «Основной», «Стратегический» и т. п.}. Объект, которому присвоено несколько категорий, содержит информацию, соответствующую этим категориям.

Множество уровней конфиденциальности образуют решетку по отношению к операции (<). Решетка (SC, $\leq$) определяется следующим образом:

SC – конечное множество уровней конфиденциальности;

$\leq$ – бинарное отношение частичного порядка для уровней конфиденциальности SC.

Отношение ($\leq$) рефлексивно ($A \leq A$), транзитивно ($A \leq B$ & $A \leq C \Rightarrow A \leq C$) и симметрично ($A \leq B$ & $B \leq A \Rightarrow A = B$).

При этом существует наибольшая верхняя граница в SC, т.е. для каждого A и B в SC существует класс $C = \max(A, B)$, такой, что:

1) $A \leq C$ и $B \leq C$;

2) $A \leq D$ и $B \leq D \Rightarrow C \leq D$ для любого D из SC.

Для каждого непустого подмножества $S = \{A_1, A_2, ..., A_n\}$ из SC существует единственный элемент $S = \max(A_1,..., A_n)$.

Можно определить также наименьшую нижнюю границу в SC. Для каждого A и B в SC существует единственный класс $E = \min(A, B)$, такой, что:

1) $E \leq A$ и $E \leq B$;

2) $D \leq A$ и $D \leq B \Rightarrow E \leq D$ для любого D из SC.

Для каждого непустого подмножества $S = \{A_1, A_2, ..., A_n\}$ из SC существует единственный элемент $S = \min(A_1,..., A_n)$.

2. Решеточная модель ценности

Решения относительно качества информации следует принимать на основе формальной модели, которая основана на следующих двух критериях: субъективной и объективной ценности.

Субъективная ценность соотносится с размером нанесенного ущерба в случае, если информация окажется известной лицам, неавторизованным для ее получения. Здесь ущерб возникает из качеств, присущих самой информации. Объективная ценность соотносится с размером нанесенного ущерба в случае, если информация окажется недоступной или имеет ненадлежащую целостность. Это – объективный критерий, зависящий от событий или спецификаций вне самой информации. Например, если финансовые документы, которые по закону должны храниться в течение ряда лет, окажутся утраченными, предприятие может быть подвергнуто штрафу.

Отдельные элементы информации согласно этой модели попадают в обе категории. Например, ведомости по персоналу, в которых указаны суммы компенсации сотрудникам, имеют субъективную и объективную ценность.

В табл. 1 приведен пример классификационной политики.

Таблица 1

Пример классификационной политики в области информации

Субъективные классификации	Метка конфиденциальности		
	Для служебного пользования	Конфиденциальная	Персональная
Определение	Раскрытие может нанести в перспективе ущерб экономике предприятия	Раскрытие может нанести серьезный ущерб экономике предприятия	Раскрытие может негативно повлиять на сотрудников или претендентов на должность
Объективные классификации	На хранении	На текущем контроле	
Определение	Ненадлежащее качество может привести в перспективе к серьезным правовым или экономическим последствиям	Ненадлежащее качество может нанести серьезный ущерб экономике предприятия	

В реальном мире существуют группы предприятий, интересы которых взаимосвязаны. Поместим их в классы конфликтных интересов. В каждом из классов находится определенное количество компаний, конкурирующих на рынке. В каждой компании, о которых было сказано выше, работают консультанты, которые имеют доступ к информации своей компании. Возможны ситуации, когда консультант из одной компа-

нии имеет доступ к сведениям других компаний. В каждой компании имеется информация, которая классифицируется на основе модели ценности. Информация содержится в объектах модели безопасности.

Опишем структуру модели безопасности и определим ее элементы, компоненты, свойства и правила. На рис. 1 изображена структура информационных ресурсов компаний.

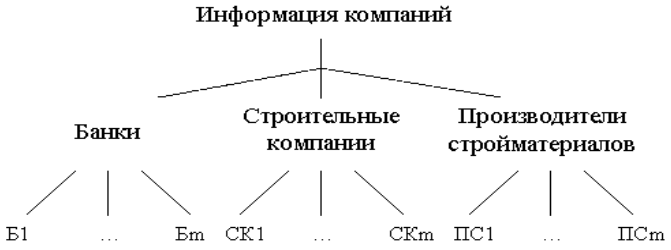

Рис. 1. Субъектная классификация информации предприятий

В каждой компании присутствует общедоступная и конфиденциальная информация. Информация делится на информацию с высоким уровнем целостности и на информацию с низким уровнем целостности (т.е. информацию, которую можно изменять). Разбиение всей информации на два уровня целостности необходимо для защиты документов от модификации, что соответствует структуре модели Биба [2].

Таким образом, объекты в данной модели описываются следующими свойствами:

- номер (или номера) компании, к которой эта информация принадлежит;
- уровень конфиденциальности (общедоступный или конфиденциальный);
- уровень целостности (низкий или высокий).

Для субъектов имеются следующие свойства:

- номера компаний, информация которых доступна субъекту;
- уровень конфиденциальности доступной информации.

Каждому субъекту и объекту в системе соответствует метка, которая отражает его свойства. Определим следующую структуру для политики безопасности:

1. Имеется несколько классов конфликтных интересов, например банки, строительные компании, производители стройматериалов.

2. Каждый класс содержит m_k компаний, как изображено на рис.1. Для каждого объекта в системе определена метка безопасности, которая представляет n-элементный вектор $\{i_1, i_2, \ldots, i_n\}$, где каждый элемент $i_k \in SC$ или $i_k = \perp$ (читается, как самый нижний) для $1 \le k \le n-2$ (последние два места отведены для атрибутов целостности и доступности). Объект, обозначенный $\{i_1, i_2, \ldots, i_n\}$, интерпретируется как содержащий информацию от компании i_1 (одного из m_1 банков), информацию от компании i_2 (одной из m_2 строительных компаний) и т.д. Если элемент вектора представляет $\perp$, то это означает, что объект не содержит критической информации ни из одной компании в соответствующем классе конфликтных интересов.

3. Пусть $S = \{s_1, s_2, ..., s_{ns}\}$, где S – множество субъектов, s_i – отдельные субъекты системы, ns – количество субъектов в системе.

Приведем пример субъекта s_1 для структуры, представленной на рис. 1: $s_1 = (1, 1, 1)$ – метка субъекта s_1, в ней содержится информация о том, что данный субъект имеет доступ к конфиденциальной информации банка 1 (Б1), строительной компании 1 (СК1), а также производителей стройматериалов 1 (ПС1).

4. Пусть $O = \{o_1, o_2, ..., o_{no}\}$, где O – множество объектов, o_i – объекты системы, no – количество объектов в системе.

Рассмотрим объект o_1 на рис. 1. Метка объекта $o_1 = (1, \perp, \perp, вц, вд)$ говорит о том, что информация этого объекта (документа) содержит конфиденциальные данные банка 1 (Б1) и не содержит конфиденциальной информации по другим классам конфликтных интересов, т.е. строительных компаний и производителей строительных материалов. Объекту присвоены метки высокой целостности и доступности.

Метки субъектов и объектов необходимы для того, чтобы можно было определить те объекты, к которым данные субъекты имеют доступ, и действия, которые они могут совершать. Все это определяют правила чтения и записи.

Правило чтения:

Субъект S может читать объект O, только если:

- метка S доминирует над меткой O.

Правило записи:

Субъект S может записывать в объект O, только если:

- метка O доминирует над меткой S.

Например, субъект s $\{2, 1, \perp\}$ может прочитать объект o $\{\perp, 1, \perp, вц, вд\}$, так как метка субъекта s доминирует над меткой объекта o и выполняется условие, разрешающее чтение. А субъект s $\{3, \perp, \perp\}$ не может прочитать объект o $\{4, 2, 1, нц, нд\}$, потому что они принадлежат разным классам конфликтных интересов.

Информация от субъекта s {2, 1, ⊥} может быть направлена в объект o {2, 1, 1, *нц*, *нд*}, потому что $o \geq s$, выполняется условие правила записи, а из субъекта s {1, 2, 3} в объект o {2, 3, 1, *нц*, *нд*} – не может, так как эти субъект и объект несопоставимы. Они не находятся в одном классе, информация принадлежит одной из конкурирующих компаний, а пользователь – другой.

Дополнительно в пределах одной компании в метке субъекта может быть добавлена роль субъекта в системе. Такая метка с записью о роли может быть использована только для потоков информации внутри одной компании, в которой назначена эта роль. Роли присваивается уникальный номер, и он указывается в метке соответствующего субъекта. Например, субъект s, соответствующий генеральному директору компании, может выглядеть следующим образом: s (1, 3, 2; 1).

Дополним это описание с учетом доступности. Как уже говорилось, закон Гроша утверждает, что ключ к увеличению отдачи от инвестиций заключается в сокращении времени доступа к информации. В таком случае необходимо размещение субъектов и объектов с высокой доступностью на высшей ступени иерархии целостности, т.е. «на текущем контроле» в модели ценности (табл. 1). В результате субъекты и объекты с высокой доступностью являются также и высокоцелостными, а компоненты с низкой доступностью не всегда являются таковыми, т.е. могут быть модифицированы. Таким образом, правила NWU (нет записи вверх) и NRD (нет чтения вниз) в структуре модели Биба соответствуют решеточной модели безопасности Белла и Лападула, так как чтение снизу высокоцелостных файлов в иерархии модели целостности Биба происходит быстро. Аналогично быстро происходит и запись информации вниз, т.е. «на хранение». В свою очередь, противоположно направленные информационные потоки, такие, как перевод информации из категории «на хранении» в категорию «на текущем контроле», и доступ высокоцелостных субъектов, в т.ч. компьютерных процессов, к программам и данным ненадлежащего качества подлежат контролю.

На рис. 2 разрешены два информационных потока: поток по записи (*write*) снизу вверх и поток по чтению сверху (*read*) – это работа с файлами операционной системы, официальными утвержденными отчетами, справочными данными и тому подобной информацией с высоким уровнем целостности. Перезапись официальной информации должна быть ограничена и строго контролироваться (NWD), поскольку она препятствует высокопроизводительной работе.

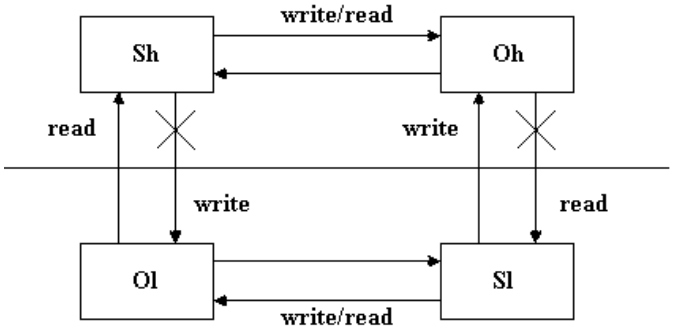

Рис. 2. Дополнение модели Белла и Лападула с учетом доступности. Высокий уровень конфиденциальности объединен с низким уровнем доступности, а низкий уровень конфиденциальности – с высоким уровнем доступности

Точно так же должен быть ограничен поток по чтению снизу (NRU) в модели Белла и Лападулы, поскольку он не только приводит к несанкционированному доступу к информации, но и замедляет высокопроизводительную обработку данных.

Процедуры коррекции информации с высоким уровнем доступа должны инициироваться записью вверх, на более конфиденциальный уровень. Таким образом, достигаются две цели: информация становится недоступной для рядовой обработки, и на более секретном уровне к ней получают доступ субъекты, которые могут ее редактировать.

Перевод информации с низкого на более высокий уровень доступности означает деклассификацию информации, т.е. ее санкционированное распространение, и должен проводиться на основе, во-первых, установления правильного форматирования и представления вновь публикуемой информации, во-вторых, проверки ее своевременности и соответствия реалиям деловых процессов и, в-третьих, под ответственность принципала, от лица которого выполняется эта операция.

Необходимо отметить, что процесс редактирования информации должен осуществляться по завершении любой иной ее обработки, в противном случае в системе одновременно окажется два «официальных» источника данных, что является нарушением.

На практике это позволяет разместить важные системные файлы в верхней части иерархии модели Биба. Это защищает доступность эталонных файлов и проверенных данных от обычных пользователей, поскольку

правило NWU не позволяет им осуществить запись в важные документы и, тем самым, исправлять официальные данные. Кроме того, если рассматривать исполнение как чтение, то высокопроизводительные процессы компьютерной системы, такие, к которым и относится закон Гроша, не могут оперировать документами и данными вне высшего круга целостности. Это обеспечивает дополнительную защиту целостности в компьютерной системе.

Данная схема обеспечивает защиту системных файлов от троянских программ. Если троянская программа находится на одном из нижних уровней в иерархии модели Биба, то она не сможет исказить системные файлы за счет правила NRD. Таким образом, осуществляется защита производительности и целостности от троянских программ. Очевидно, что такое объединение моделей может также осуществлять защиту конфиденциальности для верхних уровней определенной иерархии и защиту эффективного доступа для нижних уровней в модели Белла и Лападула.

Данная модель может объединить в себе как модель решеточного доступа (когда пользователям назначен доступ к конфиденциальным документам), так и модель дискреционного доступа (когда в матрице доступа в рамках одного предприятия может быть составлено соответствие должностей и документов, к которым пользователь, владеющий данной меткой, может иметь ограниченный доступ). Ее можно использовать при обмене информацией с другими компаниями с теми же метками, за исключением последней записи о роли субъекта, которая оставляется только для внутреннего документооборота, когда каждой роли будет соответствовать набор прав по доступу к информации. Соответствие ролей и уникальных номеров можно сохранять в таблице или матрице (табл. 2). Пример матрицы доступа приведен в табл. 3.

Таблица 2

Соответствие ролей их уникальным номерам в системе

Роль	Код
Генеральный директор	1
Заместитель директора	2
Главный бухгалтер	3

Таблица 3

Пример матрицы доступа

Роль	Права доступа	
	R	*W*
1	1	1
2	1	0
3	1	1

В матрице доступа в табл. 3 описаны права на запись *W* и на чтение *R*. Разновидность прав может быть определена, исходя из задач, которые ставятся перед пользователями. Из табл. 2 и 3, видно, например, что генеральный директор может читать и записывать в данный файл, а заместитель директора данный файл может только читать.

Матрица доступа в табл. 3 соответствует какому-то одному документу или файлу. Такая матрица должна быть создана для каждого файла, если используется дискреционная модель разграничения доступа.

3. Реализация модели

Переходим к описанию предлагаемого решения по реализации такой модели безопасности на практике. В качестве места для хранения информации об объектах и субъектах системы была выбрана база данных. Тем самым обеспечиваются все необходимые требования по обращению с информацией и пользователями, поскольку существуют готовые решения по защите баз данных и способах разграничения доступа к их ресурсам.

Опишем модель данных такой базы данных и поля таблиц, которые она будет содержать. База данных делится на две части: первая часть содержит информацию об объектах, другая часть содержит информацию о субъектах модели безопасности.

Информация каждой отдельной компании находится в отдельной таблице или таблицах, исходя из содержания такой информации. Если имеется *m* компаний в системе, тогда в общем случае имеется *m* таблиц, содержащих информацию. Приведем пример, в котором опишем структуру такой таблицы и дадим определение полей, которые должны присутствовать в обязательном порядке.

1. Идентификатор объекта – это уникальное поле, первичный ключ таблицы, необходим для того, чтобы обеспечить однозначную идентификацию записей таблицы, предотвратить повторение значений ключа, ускорить выполнение запросов к базе данных, установить связи между отдельными таблицами базы данных.

2. Принадлежность информации к другим компаниям – поле, которое содержит информацию о том, к информации какой компании имеет отношение данный объект. Уже говорилось о том, что информация в такой системе может быть доступна сотрудникам из других компаний. По значению этого поля можно судить об уровне конфиденциальности данного объекта.

3. Уровень целостности (объективный признак) – это поле, по которому можно судить о том, возможна или нет модификация объекта.

Уровень доступности – определяется уровнем целостности согласно приведенной модели безопасности.

Информация – данные, которые содержит объект.

Перечисленные выше поля таблицы являются обязательными, они обеспечивают связь объектов с субъектами. В табл. 4 содержится информация об объекте компании 1 класса конфликтных интересов 1.

Описания субъектов компании также хранятся в отдельной таблице. Таблица содержит информацию о метках безопасности субъектов, которые позволяют увидеть, к какой информации и у какого субъекта имеется доступ. Опишем значение полей, содержащихся в таблицах субъектов.

Таблица 4

Экземпляр таблицы объектов

Объекты: 1, 1
Идентификатор: 757
Принадлежность: 1,3,2
Целостность: 0
Информация: Текст
Дополнительное

1. Идентификатор субъекта – это уникальное поле, первичный ключ таблицы, он необходим для того, чтобы обеспечить однозначную идентификацию записей таблицы, предотвратить повторение значений ключа, ускорить выполнение запросов к базе данных, установить связи между отдельными таблицами базы данных.

2. Логин – уникальное имя пользователя, которое необходимо для прохождения процесса аутентификации в системе.

3. Пароль – поле, содержащее хешированное значение пароля пользователя.

4. Права доступа – поле, содержащее метку безопасности.

5. Информация – информация о пользователе, например его имя.

В табл. 5 содержится информация о субъекте компании 2 класса конфликтных интересов 2.

Таблица 5

Экземпляр таблицы субъектов

Субъекты: 2,2
Идентификатор: 867
Логин: Alex
Пароль: 1G4f~2
Метка: 1, 2, 3
Личное: Алексей

В заключение были рассмотрены существующие модели безопасности и на основе модели Брюера и Нэша [7] была построена объединенная модель безопасности, которая включила модели Белла и Лападула, Биба, контроля доступа, базирующегося на ролях, а также модели дискреционного доступа. Предложена модель ценности информации, в которой имеются только две характеристики производственной информации: субъективная, которая указывает на конфиденциальность, и объективная, которая связывает вместе целостность и доступность.

При работе над составлением требований к системе защиты использовался стандарт Банка России [3]. Это обусловлено проблемами, связанными с утечкой информации по внутренним каналам организаций, а также необходимостью защиты передаваемой информации между различными компаниями. Вместе с тем стандарт Банка России является на сегодняшний день главным документом в сфере информационной безопасности для работы организаций банковской сферы и кредитных организаций, которые и являются субъектами описываемой модели. Кроме того, стандарт рассматривает комплексно вопрос защиты и хотя и носит рекомендательный характер, но уже в ближайшем будущем, возможно, будет являться обязательным для применения. Поэтому предложенное решение включило требования по защите информации, предъявляемые стандартом безопасности Банка России.

ЛИТЕРАТУРА

1. *Олифер В.Г.*, *Олифер Н.А.* Компьютерные сети. Принципы, технологии, протоколы. Питер, 2007.
2. *Корт С.С.* Теоретические основы защиты информации: Учеб. пособие. М.: Гелиос АРВ, 2004.
3. *Стандарт* Банка России СТО БР ИББС-1.0-2006 Обеспечение информационной безопасности организаций банковской системы Российской Федерации.
4. *Зегжда П.Д.* Теория и практика обеспечения информационной безопасности. М.: Яхтсмен, 1996.
5. *LaPadula L.*, *Bell D.* Secure Computer System: Mathematical Foundation, ESD-TR-73-278. V.1, MITRE Corporation.
6. *McLean J.* Secure models, Encyclopedia of software engineering. 1994.
7. *Brewer D.F.C.*, *Nash M.J.* The Chinese Wall Security Policy: IEEE Symposium on Security and Privacy. 1989. P. 215 – 228.
8. *Gardner W.D.* Author of Grosch's Law Going Strong At 87: TechWeb Technology News: techweb.com/wire/networking/160701379/