10. *Аграновский А. В., Леднов Д. А., Репалов С. А.* Метод текстонезависимой идентификации диктора на основе индивидуальности произношения гласных звуков // Акустика и прикладная лингвистика: Ежегодник РАО. 2002. Вып. 3. С. 103–115.
11. Патент РФ № 2230375: МПК G 10 L 15/00, G 10 L 17/00. Метод распознавания диктора и устройство для его осуществления / П. В. Лабутин, А. Н. Раев, С. Л. Коваль — № 2002123509/09; заявл. 03.09.02; опубл. 10.06.04.
12. *Чистович Л. А., Венцов А. В., Грамстрем М. П. и др.* Физиология речи. Восприятие речи человеком. М.: Наука, 1976. — 388 с.

А. А. Дураковский

УПРАВЛЕНИЕ РАСПРЕДЕЛЕННОЙ СИСТЕМОЙ ЗАЩИТЫ ДОСТУПА К ДАННЫМ

Распространение вычислительных сетей предоставляет возможности для несанкционированного доступа к информационным системам (ИС), а тенденция к переходу на распределенные вычислительные системы уменьшает возможности централизованной защиты доступа к данным.

Прежде чем приступать к построению системы управления распределенной системой защиты доступа к данным, следует определить границы системы информационной безопасности [1–6]. Это можно сделать на основе следующих данных:

• структура организации — описание существующей структуры и тех изменений, которые предполагается внести в связи с разработкой системы информационной безопасности;

• размещение методов и средств вычислительной техники и поддерживающей инфраструктуры;

• ресурсы информационной системы, подлежащие защите. Рекомендуется рассмотреть ресурсы автоматизированной системы, данные, системное и прикладное программное обеспечение. Поскольку для организации все эти ресурсы представляют ценность, должна быть выбрана система критериев и методология получения оценок по этим критериям;

• технология обработки информации и решаемые задачи. Для решаемых задач следует построить модели обработки информации в терминах ресурсов.

В результате определяются технические требования к системе информационной безопасности, в которых фиксируются границы системы, перечисляются подлежащие защите ресурсы и дается система критериев для определения их ценности.

На комплексную систему технической защиты информации нормативными документами возлагается задача обеспечения функциональных свойств защищенных информационных систем. Эта задача решается как техническими, так и программными средствами базового и прикладного программного обеспечения, а также с использованием специально разрабатываемых программных и аппаратных средств технической защиты информации.

Для реализации организационно-правовых мероприятий в большинстве случаев нет необходимости использования средств, являющихся компонентами информационных систем.

Основная задача технических мероприятий — обеспечение как физической, так и информационной безопасности.

Информационная безопасность обеспечивается использованием технических средств для [7, 10]:

• построения модели защищенной системы;

• управления доступом к ресурсам информационных систем;

• обеспечения целостности и конфиденциальности;

• защиты от воздействий вирусов и иных воздействий, вызывающих любую несанкционированную модификацию информации;

• защиты информации при передаче информации.

Весь комплекс перечисленных выше проблем определяется как «политика организации безопасности на предприятии». Актуальность разработки политики информационной безопасности объясняется необходимостью формирования основ планирования информационной безопасности и управления ею на современном этапе.

Политика информационной безопасности должна охватывать следующие темы [7–10]:

• предмет, основные цели и задачи политики безопасности;

• условия применения политики безопасности и возможности ограничения;

• описание позиции законодательства в отношении выполнения политики безопасности и организации режима информационной безопасности в целом;

• права и обязанности, а также степень ответственности за выполнение политики безопасности;

• порядок действий в чрезвычайных ситуациях в случае нарушения политики безопасности.

При всем многообразии методов и подходов к защите данных практически отсутствуют методы оптимального распределения защиты по элементам данных, что позволило бы широко использовать уже разработанные методы защиты, объединив их в некоторый комплекс. Это дало бы возможность гибко организовать защиту для каждого типа данных, обеспечить повышенную защищенность и при необходимости снизить стоимость системы защиты. Таким образом, актуальной является задача разработки теоретических основ управления распределенной защитой данных на основе формального описания управления распределенной системой защиты доступа к данным в виде математической модели, а также задача определения показателей эффективности и качества распределения методов защиты по всем элементам данных.

Для формального описания распределенной системы защиты доступа к данным в виде математической модели рассмотрим взаимосвязь двух отношений A и B, где A содержит необходимые ключевые атрибуты — указатели, а B — искомую информацию, в виде направленного графа (в дальнейшем будем называть его цепочкой). Вершина A является исходной информацией, вершина B — искомой информацией, а сама цепочка — базовой.

Если все отношения защищены от несанкционированного доступа, то для доступа к информации любого отношения мы должны преодолеть некоторую защитную оболочку — капсулу (на рисунке 1 обозначена пунктиром), которую охарактеризуем, например, для вершины A как:

$$K(A)=\langle M(A), R(A), S(A), P(A)\rangle,$$

где $M(A)$ — метод защиты, $R(A)$ — способ его реализации, $S(A)$ — стоимость реализации метода, $P(A)$ — вероятность преодоления защиты, обеспеченной методом $M(A)$.

Вероятность несанкционированного преодоления защиты $P(A)$ является мерой опасности вершины.

Таким образом, чтобы найти искомую информацию в отношении B, необходимо иметь соответствующие этой информации указатели из A и открыть капсулу $K(B)$. Стрелка на отношение A, не имеющая исходящей вершины, означает, что нам не нужны указатели, достаточно лишь получить доступ к отношению A через капсулу $K(A)$. При нормальной работе с данными такой вход имеют лишь исходные вершины.

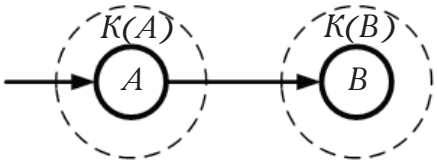

Рис. 1. Капсулированная цепочка

В предположении, что $M(A)$ и $M(B)$, соответствующие капсулам $K(A)$ и $K(B)$, независимы и не связаны между собой, меру опасности цепочки, или вероятность несанкционированного вскрытия информации по всем вершинам цепочки, определим как:

$$P(A,B)=P(A)\times P(B).$$

Действительно, доступ к информации в A и получение там указателей на поиск в B не позволяют найти необходимую информацию в B без преодоления капсулы $K(B)$. В то же время преодоление капсулы $K(B)$ и получение информации в B без преодоления капсулы $K(A)$ предоставляют нам лишь обезличенную информацию и не позволяют определить ее владельцев. Только преодоление капсул $K(A)$ и $K(B)$ одновременно дает возможность решить задачу нахождения необходимой информации. Поскольку $P(A)$ и $P(B)$ меньше единицы, то $P(A,\ B)$ меньше каждого из них.

Таким образом, разнесение отношений позволяет снизить меру опасности несанкционированного получения защищаемой информации.

Этот вывод дает возможность предложить расширенную схему защиты путем введения, например, дополнительных, так называемых ключевых вершин C и D в цепочку от A к B, содержащих только указатели на информацию в соседней вершине (рис. 2).

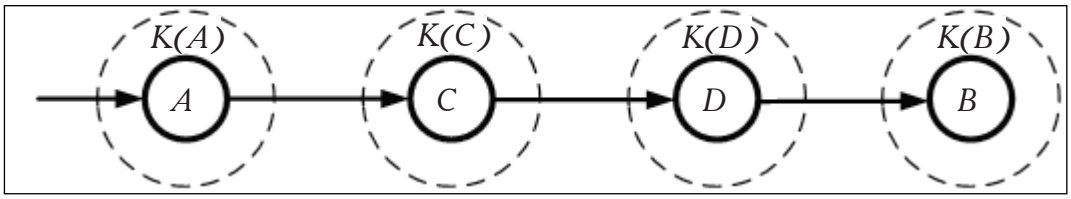

Рис. 2. Капсулированная цепочка с ключевыми вершинами

Аналогично вышеприведенному рассуждению с учетом независимости методов защиты в каждой капсуле можно вычислить меру опасности получения информации в A и B одновременно по цепочке $A,\ C,\ D,\ B$:

$$P(A,C,D,B)=P(A)\times P(C)\times P(D)\times P(B).$$

Величина $P(A,\ C,\ D,\ B)$ по определению является мерой опасности цепочки. Очевидно, что мера опасности в рассматриваемой цепочке будет меньше, чем в предыдущем случае.

Таким образом, расширение цепочки позволяет не только защитить саму информацию, но и значительно усложнить в случае несанкционированного доступа процедуру связности элементов информации между собой, поскольку получение доступа не ко всем вершинам цепочки не позволяет соотнести одни элементы информации с другими.

На основании вышеизложенного подхода алгоритм действий администратора безопасности по контролю защищенности данных в ходе обнаружения угроз безопасности в процессе эксплуатации информационной системы можно представить как методику управления распределенной системой защиты доступа к данным, включающей следующие шаги:

Шаг 1. Анализ несанкционированно преодоленных капсул. Когда администратор безопасности узнает о несанкционированном преодоления каких-либо капсул, он должен проанализировать состав преодоленных капсул, а также определить, какие методы защиты были преодолены.

Шаг 2. Построение отношений ситуативного замыкания для всех цепочек с использованием результатов теоремы о структуре ситуативного замыкания.

Шаг 3. Перерасчет мер опасности каждой цепочки на основе полученных отношений ситуативного замыкания.

Шаг 4. Сравнение полученных новых значений мер опасности со значением максимально допустимой опасности по каждой цепочке.

Шаг 5. Анализ на соответствие максимально допустимой опасности:

те цепочки, меры опасности которых укладываются в заданные ограничения, могут не подвергаться изменениям;

для цепочек, меры опасности которых превышают заданные ограничения, необходимо произвести новое распределение методов защиты, изменив состав цепочек, набор методов защиты или поменяв распределение методов по вершинам.

На рисунке 3 приведена схема методики управления распределенной системой защиты доступа к данным.

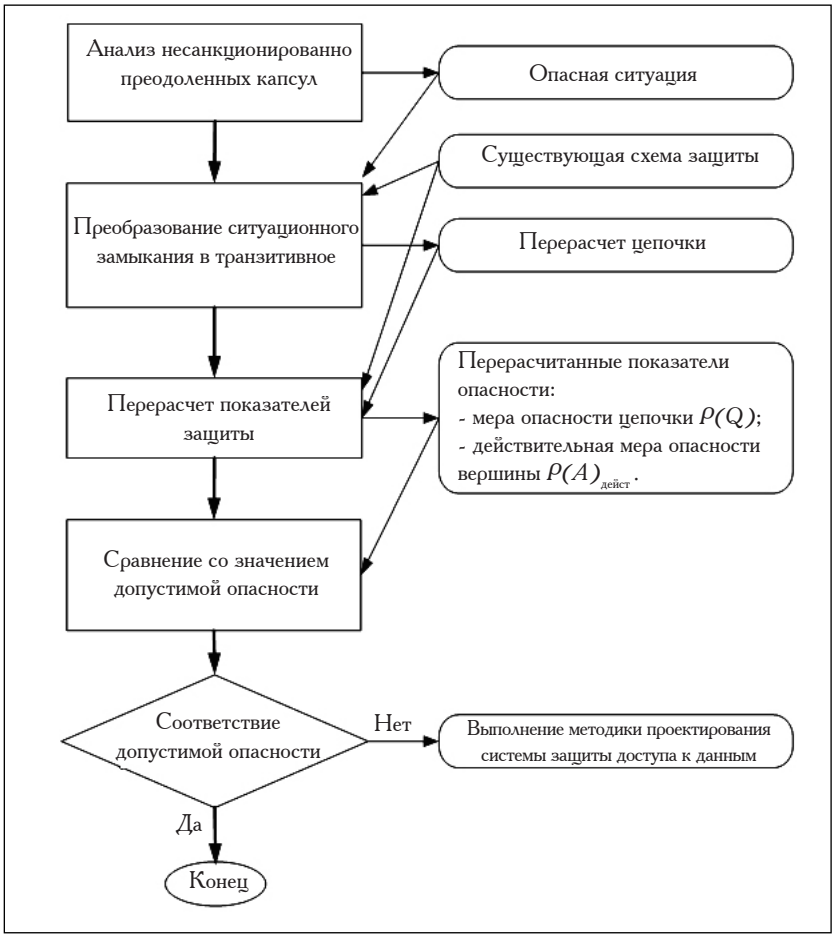

Рис. 3. Схема методики управления распределенной системой защитой доступа к данным

Представленные теоретические основы этого метода обеспечения доступа к данным построены на основе принципа распределенной защиты. При этом доступ к связанным данным определяется преодолением линейной последовательности защищенных данных и ключевых отношений. Распределение защит по цепочке позволяет усилить общую защиту данных при одновременном упрощении процесса защиты.

СПИСОК ЛИТЕРАТУРЫ:

1. *Герасименко В. А.* Защита информации в автоматизированных системах обработки данных: в 2 т. М.: Энергоатомиздат, 1994.
2. *Минаев В. А., Фисун А. П., Скрыль С. В., Дворянкин С. В., Никитин М. М., Хохлов Н. С.* Информатика: концептуальные основы. М.: Маросейка, 2008.
3. *Минаев В. А., Фисун А. П., Скрыль С. В., Дворянкин С. В., Никитин М. М., Хохлов Н. С.* Информатика: Средства и системы обработки данных. М.: Маросейка, 2008.
4. *Кузнецов Н. А., Кульба В. В., Микрин Е. А. и др.* Информационная безопасность систем организационного управления. Теоретические основы: в 2 т. М.: Наука, 2006.

5. Руководящий документ. Безопасность информационных технологий: Руководство по разработке профилей защиты и заданий по безопасности. М.: Гостехкомиссия России, 2003.
6. Руководящий документ. Безопасность информационных технологий: Критерии оценки безопасности информационных технологий. М.: Гостехкомиссия России, 2002. Части 1, 2, 3.
7. *Домарев В. В.* Безопасность информационных технологий: системный подход. М.: ООО «ТИД «ДС», 2004.
8. *Петренко С. А., Курбатов В. А.* Политика информационной безопасности. М.: Компания «АйТи», 2006.
9. *Черненький В. М.* Проблемы информационной безопасности в банковских системах: Учеб. пособие. М.: ООО «Элвис+», 2003.
10. *Ярочкин В. И.* Информационная безопасность. М.: Академический проект, 2004.