УДК 316.4

Т.В. Карлова, Н.М. Кузнецова

СОЦИОДИНАМИЧЕСКАЯ МОДЕЛЬ АВТОМАТИЗИРОВАННОГО УПРАВЛЕНИЯ РАЗГРАНИЧЕНИЕМ ДОСТУПА К ИНФОРМАЦИОННЫМ И ПРОГРАММНЫМ РЕСУРСАМ ПРОМЫШЛЕННОГО ПРЕДПРИЯТИЯ

Представлена социодинамическая модель автоматизированного управления разграничением доступа к конфиденциальному информационному и программному обеспечению, которая может быть использована на промышленных предприятиях, а также в организациях, располагающих конфиденциальными информационными и программными ресурсами.

Ключевые слова: социодинамика, автоматизация, разграничение доступа, защита информации, программное обеспечение, информационные ресурсы.

Увеличение количества видов хакерских атак, повышение сложности автоматизированных систем промышленных предприятий, а также широкое использование электронного документооборота требуют применения более усовершенствованных технологий защиты информационного и программного обеспечения, в том числе методов разграничения доступа.

В рамках предлагаемой модели всех участников информационных отношений предприятия необходимо разделить на субъекты и объекты.

К субъектам относятся:

– сотрудники промышленного предприятия;

– представители третьей стороны.

Примером представителей третьей стороны могут служить аудиторы, консультанты – сотрудники других организаций, принимающие участие в информационных отношениях предприятия.

К объектам относятся информационные и программные ресурсы предприятия:

– базы данных;

– приложения;

– сервисы;

– файловые системы;

– электронные архивы.

Главной задачей модели является обеспечение автоматизированного разграничения доступа субъектов информационных отношений к соответствующим объектам [1].

На промышленном предприятии должны быть определены уровни доступа к ресурсам. Данное разграничение может осуществляться согласно классификации ресурсов по грифам секретности, важности, полезности и т.д.

На рис. 1 представлена модель информационных отношений промышленного предприятия.

Количество уровней доступа не должно быть слишком большим, так как это может привести к потере эффективности работы основной автоматизированной системы предприятия. С другой стороны, количество уровней доступа должно быть достаточным для сохранения требуемых параметров информационной защиты.

Уровни доступа к информационным и программным ресурсам могут формироваться тремя методами:

1. Назначение списка прав доступа для каждого уровня. Является аналогом дискреционной модели разграничения доступа.

2. Формирование иерархии прав доступа. Является аналогом мандатной модели разграничения доступа.

3. Гибридное использование метода 1 и метода 2.

Рис. 1. Модель управления информационными отношениями промышленного предприятия

Структуры методов представлены на рис. 2, 3, 4 соответственно.

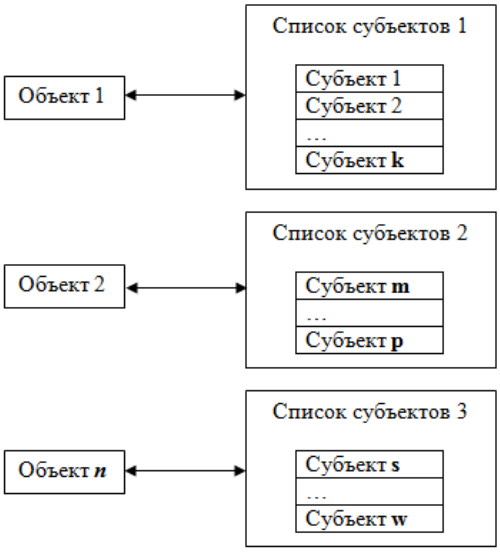

Рис. 2. Назначение списка прав доступа

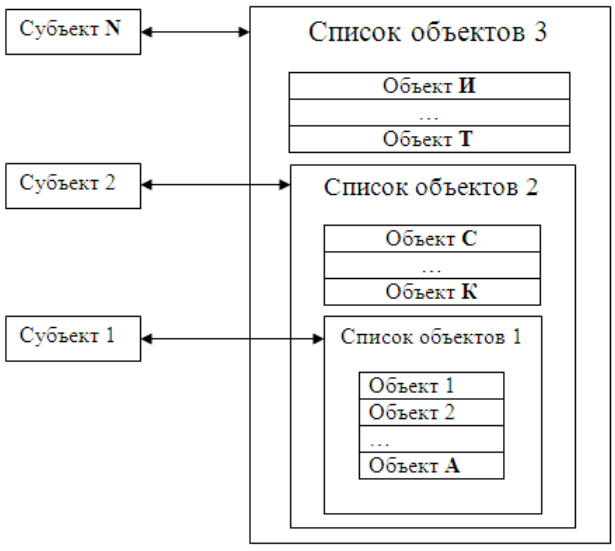

Рис. 3. Иерархия прав доступа

При использовании первого метода назначение прав доступа осуществляется путём формирования списка допущенных субъектов для каждого объекта информационных отношений. Подобная процедура выполняется при формировании так называемого списка DACL (Discretionary Access Control List) - списка разграничительного контроля доступа дискреционной модели [2; 3].

Таким образом, уровни доступа формируются относительно объектов информационных отношений.

Следует отметить, что списки субъектов могут являться пересекающимися множествами, поэтому к одному объекту могут иметь доступ сразу несколько субъектов.

При использовании второго метода назначение прав доступа осуществляется путём формирования иерархической структуры уровней прав доступа таким образом, чтобы субъект, имеющий более высокий уровень доступа, был наделен правами, соответствующими всем более низким уровням доступа.

Уровни доступа формируются относительно субъектов информационных отношений.

Согласно рис. 3, субъект 1 имеет минимальный набор прав доступа, субъект N обладает всеми правами доступа. Важно отметить, что списки объектов являются вложенными множествами.

Применение гибридного метода предполагает формирование сложной иерархической структуры списков прав доступа. При использовании данного метода необходимо тщательное ознакомление с инфраструктурой, основной информационной системой предприятия, с принятой на предприятии политикой безопасности. Достоинством данного метода является высокий уровень надёжности, недостатками – сложность реализации, низкий уровень гибкости, влияние на функционирование основной информационной системы предприятия.

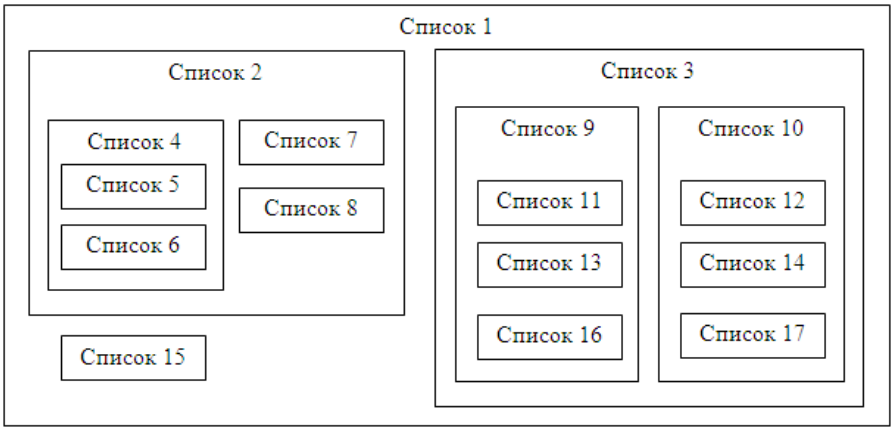

Рис. 4. Иерархия списков прав доступа

На рис. 5 представлены диаграммы Эйлера субъектов информационных отношений для каждого из перечисленных методов.

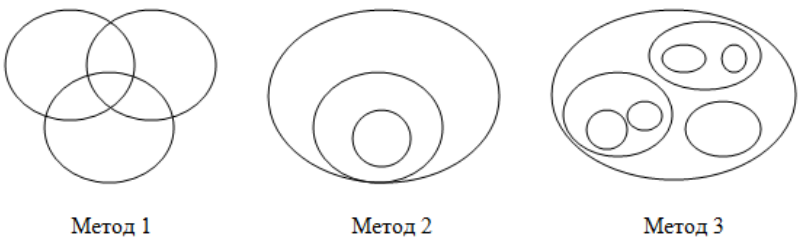

Рис. 5. Диаграммы Эйлера для методов формирования списков субъектов доступа

Применение описанных методов формирования списков доступа и социодинамической модели автоматизированного управления разграничением доступа повысит уровень информационной безопасности промышленного предприятия.

СПИСОК ЛИТЕРАТУРЫ

1. Карлова, Т.В. Разработка концепции обеспечения многоуровневого доступа к конфиденциальной информации / Т.В. Карлова, Н.М. Кузнецова // Вестн. МГТУ «Станкин». - 2011. - № 2 (14). - С. 87-90.
2. Хорев, П.Б. Методы и средства защиты информации в компьютерных системах: учеб. пособие для студентов высш. учеб. заведений / П.Б. Хорев. - М.: Академия, 2005. - 256 с.
3. Мельников, В. П. Информационная безопасность и защита информации: учеб. пособие для студентов высш. учеб. заведений / В. П. Мельников, С. А. Клейменов, А. М. Петраков; под ред. С. А. Клейменова. - М.: Академия, 2008. - 336 с.

Материал поступил в редколлегию 18.07.14.