3. *CreateR*(*r*) — создает роль *r* — добавляет в граф вершину, не связанную с другими вершинами. Данный оператор сам по себе никак не влияет на распределение привилегий и не может приводить к нарушению безопасности.

4. *DeleteR*(*r*) — удаляет роль *r* — удаляет в графе вершину. Условием выполнения оператора является изолированность вершины. Для удаления вершины со связями необходимо предварительно удалить все дуги с помощью оператора *DeleteA*( ). Как легко понять, данный оператор сам по себе также не приводит к перераспределению полномочий.

5. *EnterP*(ρ, *r*) — добавляет привилегию ρ в множество привилегий роли *r*. Соответственно, данная привилегия также добавляется всем ролям, доминирующим над данной ролью.

6. *DeleteP*(ρ, *r*) — удаляет привилегию ρ из множества привилегий роли *r*. Соответственно, привилегия ρ удаляется также и у ролей, доминирующих над *r*, если они не наследуют эту привилегию от других ролей.

Для выполнения сложных преобразований системы из элементарных операторов могут быть составлены команды: *Command C* $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ ($\alpha_1, \alpha_2, \ldots, \alpha_n$ — элементарные операторы).

Доказательство следующего утверждения сводится к подбору требуемой последовательности элементарных операторов.

Предложение 5. Для любых двух ролевых графов *G* и *G′* существует команда *C*, преобразующая *G* в *G′*.

Исходя из этого утверждения описанный выше набор элементарных операторов является полным и на его основе можно построить любой ролевой граф.

Таким образом, для ролевой политики безопасности имеется возможность формализации путем определения элементарных операторов преобразования ролевого графа. Их использование, в свою очередь, позволит получать более строгие доказательства безопасности систем с ролевым разграничением доступа к информации в соответствии с определенными формализованными критериями.

СПИСОК ЛИТЕРАТУРЫ:

1. *Гайдамакин Н. А.* Разграничение доступа к информации в компьютерных системах. Екатеринбург: Изд-во Урал. ун-та, 2003. — 328 с.

2. *Новиков Ф. А.* Дискретная математика для программистов. СПб.: Питер, 2001. — 304 с.

3. *Белим С. В., Богаченко Н. Ф., Ракицкий Ю. С.* Совмещение ролевой и мандатной политик безопасности // Проблемы обработки и защиты информации. Книга 1. Модели политик безопасности компьютерных систем. Коллективная монография / Под общей ред. д.ф.-м.н. С. В. Белима. Омск: ООО «Полиграфический центр КАН», 2010. С. 117–132.

Е. А. Беляева

ОСНОВНЫЕ ПОДХОДЫ К ТЕСТИРОВАНИЮ МНОГОФУНКЦИОНАЛЬНЫХ АППАРАТНО-ПРОГРАММНЫХ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

Проблема обеспечения защиты информации, обрабатывающейся автоматизированными системами в защищенном исполнении (АС ЗИ), от НСД является одной из важнейших проблем современного общества [1].

При создании и эксплуатации АС ЗИ, предназначенных для обработки информации, содержащей государственную тайну, в соответствии с требованиями руководящих документов ФСБ РФ по защите информации необходимо применять специальный класс аппаратно-программных средств защиты информации – АПМДЗ.

Основными функциями АПМДЗ являются:

- идентификация и аутентификация пользователей;
- контроль целостности программного обеспечения и других объектов файловой системы ПЭВМ, в которой установлен АПМДЗ;
- блокировка загрузки нештатной копии операционной системы;
- ведение журнала событий.

Однако наряду с перечисленными выше основными функциями АПМДЗ предприятия-разработчики подобных устройств зачастую реализуют на плате АПМДЗ ряд дополнительных устройств, например:

- канальные шифраторы;
- шифраторы сменных носителей информации;
- защищенные доверенные хранилища информации;
- доверенные сетевые адаптеры с возможностью обеспечения односторонней передачи информации.

Расширение функциональных возможностей АМПДЗ и создание на их основе многофункциональных аппаратно-программных средств защиты информации обуславливают необходимость проведения исследований подобных устройств на предмет оценивания корректности и надежности реализации дополнительных функциональных возможностей АМПДЗ в свете их влияния на функциональную безопасность АС ЗИ в целом.

Для повышения функциональной безопасности АС ЗИ необходимо разработать методику комплексного тестирования многофункциональных аппаратно-программных средств защиты информации на базе АПМДЗ, позволяющую оценить функциональную безопасность и обеспечить требуемый уровень защищенности от НСД.

В целях решения поставленной задачи будут разработаны частные методики тестирования различных функциональных подсистем многофункциональных аппаратно-программных средств защиты информации, обеспечивающие оценивание уровня функциональной безопасности всего устройства, в зависимости от архитектуры построения функциональных подсистем и параметров их настроек; обоснованы наборы тестируемых характеристик, в зависимости от назначения той или иной функциональной подсистемы, влияющие на уровень функциональной безопасности.

Для выбора устройства АПМДЗ, предлагаемого к применению в АС ЗИ, будут проводиться испытания на основании разработанных методик, по итогам которых будет выбран показавший наилучшую результативность по испытаниям АПМДЗ модуль.

СПИСОК ЛИТЕРАТУРЫ:

1. Доктрина информационной безопасности Российской Федерации. Утверждена Президентом Российской Федерации 9 сентября 2000 г. № Пр-1895.

2. *Романец Ю. В., Тимофеев П. А., Шаньгин В. Ф.* Защита информации в компьютерных системах и сетях / Под ред. В. Ф. Шаньгина. 2-е изд., перераб. и доп. М.: Радио и связь, 2001.