Аналогичного мнения придерживается и Д. В. Добровольский, который предлагает декриминализировать статью 274 УК РФ путем исключения ее из УК РФ, так как отсутствует реальная необходимость в уголовной наказуемости такого отклоняющегося поведения [9].

Е. В. Красненкова предлагает конкретизировать диспозицию рассматриваемой статьи и изложить ее как «нарушение правил эксплуатации компьютерных и иных автоматизированных электронных систем обработки данных, а также их сетей и систем». Такой подход представляется вполне оправданным, так как он учитывает устоявшуюся сегодня терминологию в сфере безопасности информационных технологий [10].

В связи с вышесказанным, мы предлагаем свое видение рассматриваемой статьи, изложенной в следующей редакции:

«Статья 274. Нарушение работы информационно-телекоммуникационных устройств, их систем и сетей

1. Нарушение работы информационно-телекоммуникационных устройств, их систем и сетей, повлекшее уничтожение, блокирование или модификацию охраняемой законом цифровой информации, — наказывается ...»

СПИСОК ЛИТЕРАТУРЫ:

1. *Дворецкий М. Ю., Копырюлин А. Н.* Правоприменение ст. 274 Уголовного кодекса РФ // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2008. № 2. С. 495.
2. *Кузнецов А. П.* Ответственность за нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети // Правовые вопросы связи. 2007. № 2. С. 25–29.
3. *Сизов А. В.* Квалификация нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети // Информационное право. 2007. № 4. С. 27–30.
4. *Кабанова А. Ж.* Преступления в сфере компьютерной информации (уголовно правовые и криминологические аспекты). Автореф. дис. … канд. юрид. наук. Ростов-на-Дону, 2004. С. 6.
5. *Скляров Д. В.* Искусство защиты и взлома информации. СПб.: БХВ-Петербург, 2004. С. 10.
6. *Зинина У. В.* Преступления в сфере компьютерной информации в российском и зарубежном праве. Автореф. дис. … канд. юрид. наук. М., 2007. С. 14.
7. *Тропина Т. Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы. Автореф. дис. … канд. юрид. наук. Владивосток, 2005. С. 11.
8. *Зубова М. А.* Компьютерная информация как объект уголовно-правовой охраны. Автореф. дис. … канд. юрид. наук. Казань, 2008. С. 14.
9. *Добровольский Д. В.* Актуальные проблемы борьбы с компьютерной преступностью. Автореф. дис. … канд. юрид. наук. М., 2005. С. 9.
10. *Красненкова Е. В.* Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами. Автореф. дис. … канд. юрид. наук. М., 2006. С. 10.

С. В. Белим, Н. Ф. Богаченко

ГРАФ ВЛИЯНИЯ И ЭЛЕМЕНТАРНЫЕ ОПЕРАТОРЫ РОЛЕВОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ

Ролевое разграничение доступа к информации получило широкое распространение не только в системах управления базами данных, но и в операционных системах. Основное отличие ролевой политики безопасности от мандатной и дискреционной состоит в управлении привилегиями. Под привилегией понимается возможность осуществления некоторых действий в системе в целом. Ролевую политику

безопасности принято анализировать исходя из иерархии ролей, наиболее удобным представлением которой являются ориентированные графы, называемые далее ролевыми графами. Однако на сегодняшний день отсутствует формальный подход, позволяющий отслеживать преобразования ролевого графа. Данная работа закладывает основу для создания модели ролевого разграничения доступа исходя из набора примитивных операторов, по аналогии с моделью HRU [1].

Будем считать, что в системе задано некоторое множество ролей R, наделенных привилегиями из множества P (множества R и P конечны). Иерархия ролей определена ориентированным графом $G(R, A)$: вершины R данного графа соответствуют ролям, дуги A задают отношение авторизации (авторизация одной роли на другую подразумевает полное наследование ее привилегий). При этом, если в графе имеется дуга (r, r'), значит, роль r авторизована на роль r'. Очевидно, что роль r может унаследовать только привилегии ролей r', связанных с ней ориентированными путями $\rho(r, r')$. Введем обозначение для множества ролей, до которых существует путь от вершины r в ролевом графе G: $PR(r) = \{r' \mid \exists\ \rho(r, r')\}$ — множество тех ролей, от которых привилегии передаются роли r.

Перейдем теперь к вопросам безопасности системы с ролевым разграничением доступа. Будем считать, что происходит *утечка привилегии* ρ, если роль r получает ее несанкционированно. Система с ролевым разграничением доступа *безопасна*, если в ней не происходит утечка привилегий. Следует отметить, что данное выше определение безопасности является алгоритмическим. По сути, *система будет безопасной, если возможна реализация алгоритма, следящего за передачей привилегий в системе*. Задача проверки безопасности системы сводится к исследованию возможности передачи привилегий по дугам графа.

Как было сказано выше, привилегии роли r могут передаваться только от ролей из множества $PR(r)$, т. е. роли из множества $PR(r)$ *влияют* на r. Будем говорить, что роль r' *не влияет* на роль r, если добавление любой привилегии ρ в множество привилегий роли r' не приводит к изменению множества привилегий роли r. Легко понять, что роли из множества $R \setminus PR(r)$ не влияют на роль r. Далее, подграф $GR(r)$ ролевого графа G, вершинами которого является множество $PR(r)$, а дугами — соответствующие дуги между этими вершинами из графа G, будем называть *графом влияния* на роль r. Таким образом, для анализа безопасности системы необходимо отслеживать передачу привилегий по графам влияния. Используя свойства ориентированных деревьев и адаптируя алгоритмы поиска на графах [2], можно доказать следующий ряд утверждений.

Предложение 1. Если ролевой граф G является деревом, то граф влияния $GR(r)$ на произвольную роль r также будет деревом.

Предложение 2. Если ролевой граф G является решеточным (порождает решетку [3]), то граф влияния $GR(r)$ на произвольную роль r также будет решеточным.

Предложение 3. Трудоемкость поиска графа влияния на произвольную роль не превосходит $O(n^2)$.

Предложение 4. Если в системе ролевое дерево неизменно, то система является безопасной.

Пусть теперь ролевое дерево может изменяться в процессе функционирования системы. Для анализа этих преобразований введем набор элементарных операторов, преобразующих граф G.

1. $Auth(r_1, r_2)$ — авторизация роли r_1 на роль r_2 — добавляет дугу от r_1 к r_2. Данная операция приводит к тому, что множество привилегий роли r_1 (обозначим его $r_1.\rho$) изменяется и становится равным $r_1.\rho \cup r_2.\rho$, множество привилегий $r_2.\rho$ роли r_2 остается неизменным.

2. $DeleteA(r_1, r_2)$ — отменяет авторизацию роли r_1 на роль r_2 — удаляет дугу от r_1 к r_2. Новое множество привилегий роли r_1 имеет вид $(r_1.\rho \setminus r_2.\rho) \cup S$ ($S = \bigcup r'.\rho$, при этом объединение берется по всем r', принадлежащим множеству $PR(r_1) \setminus r_2$). Простая разность множеств привилегий $r_1.\rho \setminus r_2.\rho$ может приводить к неверному результату, так как возможна ситуация, когда одна и та же привилегия наследуется от нескольких ролей.

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].