E. E. Yandybaeva, I. V. Mashkina

Methods of Information Subjects and Objects Interaction Rules Formalization in the Electronic Trading Platform System

Key words: electronic trading platform, mandatory role-based access control, roles hierarchy, access rights

The methods of information subjects and objects interaction rules formalization in the electronic trading platform system has been developed. They are based on mathematical model of mandatory role-based access control. As a result of the work we have defined set of user roles and constructed roles hierarchy. For the roles hierarchy restrictions have been imposed to ensure the safety of the information system.

Э. Э. Яндыбаева, И. В. Машкина

МЕТОДИКА ФОРМАЛИЗАЦИИ ПРАВИЛ ВЗАИМОДЕЙСТВИЯ ИНФОРМАЦИОННЫХ СУБЪЕКТОВ И ОБЪЕКТОВ В СИСТЕМЕ ЭЛЕКТРОННОЙ ТОРГОВОЙ ПЛОЩАДКИ

В настоящей работе в качестве объекта защиты рассматривается информационная система (ИС) электронной торговой площадки (ЭТП). Целью работы является формализованное описание правил взаимодействия информационных субъектов и объектов в ИС ЭТП с помощью математической модели мандатного ролевого разграничения доступа. Основными элементами данной математической модели являются [1]:

U — множество пользователей;

R — множество ролей;

P — множество прав доступа к объектам;

S — множество сессий пользователей;

(L, ≤) — решетка уровней конфиденциальности информации;

PA: $R \to 2^P$ — функция, определяющая для каждой роли множество прав доступа, при этом для каждого $p \in P$ существует $r \in R$, такая, что $p \in PA(r)$;

UA: $U \to 2^R$ — функция, определяющая для каждого пользователя множество ролей, на которые он может быть авторизован;

roles: $S \to 2^R \cup 2^{AR}$ — функция, определяющая для пользователя множество ролей, на которые он авторизован в данной сессии, при этом в каждый момент времени для каждого $s \in S$ выполняется условие $roles(s) \subseteq UA(user(s)) \cup UA(user(s))$;

c: $U \to L$ — функция уровня доступа пользователя;

c: $O \to L$ — функция уровня конфиденциальности объекта;

A = {read, write} — виды доступа.

Данная математическая модель адаптирована для исследуемого объекта защиты — ИС ЭТП. На первом этапе для ИС ЭТП определено множество объектов доступа, каждому из которых присвоены уровни конфиденциальности, определено множество ролей пользователей и их уровни доступа. Множество ролей пользователей ИС ЭТП включает следующие роли:

r1 — внешнее по отношению к оператору ЭТП лицо, не зарегистрированное в ИС ЭТП;

r2 — работник клиента ЭТП с правом объявления аукциона и правом подачи заявки на участие в торгах;

r3 — работник клиента ЭТП с правом подписания контракта;

r4 — работник клиента ЭТП с правами администратора личного кабинета;

r5 — работник оператора ЭТП;

r6 — администратор ЭТП;

r7 — топ-менеджер оператора ЭТП;

r8 — работник компании, осуществляющей внедрение и сопровождение программного обеспечения ИС ЭТП;

r9 — работник компании, осуществляющей ремонт технических средств ИС ЭТП.

Далее на определенном для ИС ЭТП множестве ролей пользователей сформирована иерархическая структура ролей пользователей ИС ЭТП [2]. Иерархия ролей пользователей ИС ЭТП задает на множестве R отношение частичного порядка «≤», при котором выполняется условие: для $u \in U$, если $r_i, r_j \in R$, $r_j \in UA(u)$ и $r_i \le r_j$, то $r_i \in UA(u)$. При этом для $r_i \le r_j$ выполняется одно из условий: 1) $r_i = x_i\_read$, $r_j = x_j\_read$, $x_i \le x_j$; 2) $r_i = x_i\_write$, $r_j = x_j\_write$, $x_j \le x_i$.

Для иерархии ролей пользователей ИС ЭТП выполняются следующие ограничения:

- ограничение функции UA() — для каждого пользователя $u \in U$ роль $x\_read = \oplus (UA(u) \cap \{y\_read \mid y \in L\})$ $UA(u)$ (здесь $x = c(u)$) и $x\_write = \oplus\{y\_write \mid y \in L\} \in UA(u)$ (здесь $x = \otimes L$);
- ограничения функции roles() — для каждой сессии $s \in S$ множество ролей $roles(s) = \{x\_read, x\_write\}$;
- ограничения функции PA() — должно выполняться:
- для каждого $x \in L$ доступ $(o, read) \in PA(x\_read)$ тогда и только тогда, когда доступ $(o, write) \in PA(x\_write)$;
- для каждого доступа (o, read) существует единственная роль x_read: $(o, read) \in PA(x\_read)$ (здесь $x = c(o)$).

Из вышеперечисленного следует, что соблюдаются требования либерального мандатного разграничения доступа. Согласно [1], если модель взаимодействия информационных субъектов и объектов соответствует либеральному или строгому мандатному разграничению доступа, то в ней для $o_i, o_j \in O$, таких, что $c(o_i) > c(o_j)$, невозможно возникновение информационных потоков от o_i к o_j. Это означает, что невозможна утечка конфиденциальной информации.

С учетом приведенных выше условий и ограничений разработана матрица доступа ролей пользователей ИС ЭТП к множеству объектов доступа.

На следующем этапе работы определено множество административных ролей ИС ЭТП. На данном множестве также реализована иерархическая структура. Все административные роли ИС ЭТП предназначены для администрирования множеств авторизованных ролей пользователей и администрирования множеств прав доступа, которыми обладают роли. Часть административных ролей ИС ЭТП дополнительно наделены правами администрирования иерархии ролей пользователей. Правила администрирования сформированы и представлены в виде рассчитанных значений функций can-assign, can-revoke, $can\text{-}assign_\rho$, $can\text{-}revoke_\rho$, $can\text{-}assign_a$, $can\text{-}revoke_a$, $can\text{-}assign_g$ и $can\text{-}revoke_g$.

На основе разработанной методики формализации правил взаимодействия информационных субъектов и объектов формируются локальные политики безопасности для ИС ЭТП, реализуемые в используемых на исследуемом объекте средствах защиты информации. Благодаря использованной в работе математической модели мандатного ролевого разграничения доступа в разработанной методике отсутствуют противоречия и возможно теоретическое доказательство безопасности ИС ЭТП как объекта защиты.

СПИСОК ЛИТЕРАТУРЫ:

1. *Девянин П. Н.* Модели безопасности компьютерных систем: Учеб. пособие для студ. высш. учеб. заведений. М.: Издательский центр «Академия», 2005. — 144 с.
2. *Яндыбаева Э. Э., Машкина И. В.* Политика контроля доступа в информационной системе электронной торговой площадки // Информационное противодействие угрозам терроризма. Научно-практический журнал. 2014. № 23. С. 189–194.

REFERENCES:

1. *Devyanin P. N.* Modeli bezopasnosti kompyuternyh system. M.: Akademiya, 2005.
2. *Yandybaeva E. E., Mashkina I. V.* Politika kontrolya dostupa v informatsionnoy sisteme electronnoy torgovoy ploshchadki // Information counteraction to the terrorism threat. Scientific and practical journal. 2014. № 23. P. 189–194.