МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
ОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ им. Ф.М. ДОСТОЕВСКОГО

ОМСКИЕ НАУЧНЫЕ ЧТЕНИЯ

Материалы Всероссийской научно-практической конференции

(Омск, 11–16 декабря 2017 г.)

ISBN 978-5-7779-2192-5

Омск

ИЗДАТЕЛЬСТВО ОМСКОГО ГОСУДАРСТВЕННОГО УНИВЕРСИТЕТА

2017

ВЫЯВЛЕНИЕ ЦЕНЫ ПСИХОЛОГИЧЕСКОЙ ОШИБКИ АДМИНИСТРАТОРА КОМПЬЮТЕРНОЙ СЕТИ В ОЦЕНКЕ КВАЛИФИКАЦИИ ЗЛОУМЫШЛЕННИКОВ

THE PRICING PSYCHOLOGICAL ERRORS OF THE COMPUTER NETWORK ADMINISTRATOR TO ASSESS OF THE CYBER CRIMINALS SKILLS

А.К. Гуц
A.K. Guts
Омский государственный университет им. Ф.М. Достоевского
Dostoevsky Omsk State University

С помощью теории рефлексивных игр демонстрируется, как психологические ошибки системных администраторов могут сказаться на защите компьютерных сетей.

With the help of the theory of reflexive games one is demonstrated how psychological errors system administrators can affect on the defense of computer networks.

Ключевые слова: защита компьютерных сетей, рефлексивные игры, психология системного администратора.

Keywords: defense of computer networks, reflexive games, system administrator psychology.

Представим, что в атаке на компьютерную сеть участвуют два злоумышленника, уверенные в своих силах, а администратор сети не имеет должной квалификации и более того, не считает злоумышленников серьезными противниками. При этом оба злоумышленника хорошо информированы об администраторе и его действиях, а он не имеет о них необходимой информации.

Обозначим через x_i – усилия, предпринимаемые участниками рассматриваемой ситуации, причем x_1 и x_2 – это действия злоумышленников, а x_3 – действия администратора. Добавим двух фантомных участников: пусть x_{31} и x_{32} описывают действия образов 1-го и 2-го злоумышленника в представлении о них администратора. Администратор считает, что он и его противники, а точнее фантомные участники, одинаково информированы о ситуации. На рис. 1 дан граф информированности всех участников.

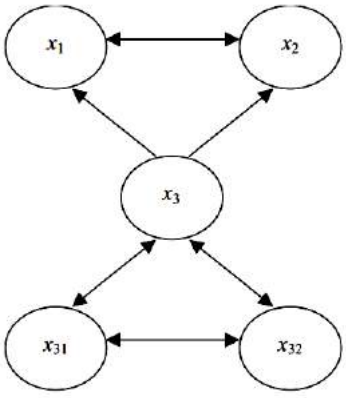

Рис. 1

Какими будут усилия всех участников ситуации, и кто более усердствует, злоумышленники или администратор и, следовательно, у кого больше шансов добиться своей цели?

Для ответа на данный вопрос воспользуемся теорией рефлексивных игр, изложенной в [1], а также примером их этой книги, данным на [1, с. 77, 80].

Введем следующие целевые функции пяти участников:

$$f_i(\theta - x_1 - x_2 - x_3)x_i - \frac{1}{2}x_i^2 \ (i = 1, 2, 3),$$

$$f_j(\theta - x_3 - x_{31} - x_{32})x_j - \frac{1}{2}x_j^2 \ (j = 3, 31, 32).$$

Здесь θ = 1 или 2 в зависимости от уверенности в своих силах и квалификации. Злоумышленники уверены в своем всесилии, поэтому для них выбираем значение θ = 2. А вот квалификация администратора не на должной высоте, и он не оценивает должным образом квалификацию злоумышленников. Поэтому для него и для фантомных участников берем θ = 1.

Находим информационное равновесие (формула (41) из [1]) для пяти участников, как реальных, так и фантомных, являющееся аналогом равновесия Нэша. Имеем пять уравнений (см.: [1, с. 80])

$$\frac{\partial}{\partial x_i} f_i = 0 \ (i = 1, 2, 3, 31, 32),$$

из которых находим оптимальные усилия, затрачиваемы на атаку и соответственно на защиту злоумышленников и администратора:

$$x_1^* = \frac{9}{20}, x_2^* = \frac{9}{20}, x_3^* = \frac{1}{5}, x_{31}^* = \frac{1}{5}, x_{32}^* = \frac{1}{5}.$$

Как видим, злоумышленники настроены более решительно (9/20>1/5) и их действия более успешны, если принять, что большее значение величины x_i означает лучшие шансы на успех. Правда, приведенные значения x_i^* обеспечивают некоторое равновесие сил, когда еще злоумышленники не одержали перевеса в борьбе с администратором, и принятые им меры защиты пока еще действенны. Итог борьбы зависит от того, у кого есть ресурсы для продолжения противостояния.

Если бы информированность всех трех реальных участников была одинаковой (рис. 2), то фантомных участников не было бы (администратору нет необходимости порождать их, поскольку он и так все знает о злоумышленниках), и мы имели бы следующие значения для усилий трех участников $x_1^* = \frac{1}{2}, x_2^* = \frac{1}{2}, x_3^* = 0$ при информационном равновесии, которое в данном случае совпадает с классическим равновесием Нэша [1, с. 74]. Мы видим, что отсутствие информированности о злоумышленниках заставляет администратора рефлексировать, порождать фантомных соперников, и это ведет к тому, что он затрачивает дополнительные усилия (1/5>0), в то время как усилия злоумышленников снижаются (9/20 <1/2).

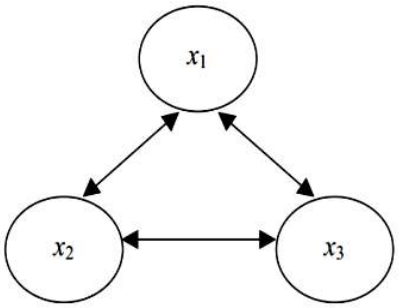

Рис. 2

Отметим, что поддержание классического равновесия Нэша – это в какой-то мере учет интересов злоумышленников; во всяком случае администратор знает о них, и поэтому соблюдение интересов злоумышленников находится на грани допустимого с точки зрения российского законодательства [2].

Поскольку в реальности знания о злоумышленниках не являются полными, то администратор ведет с ними рефлексивную игру, имея шанс на успех своих мер защиты, как это происходит в случае установления информационного равновесия, даже в случае недооценки квалификации злоумышленников. При этом администратора трудно обвинить в халатности.

1. *Новиков Д.А., Чхартишвили А.Г.* Рефлексивные игры. М.: СИНТЕГ, 2003. 149 с.

2. *Гуц А.К.* Теория игр, равновесия Нэша и законодательство в сфере компьютерных преступлений // Математическое и компьютерное моделирование: сб. материалов науч. конф. (18 октября 2013 г.). Омск: ОмГУ, 2013. С. 8–9.

Сведения об авторе:

Гуц Александр Константинович – д-р физ.-мат. наук, профессор кафедры кибернетики ОмГУ им. Ф.М. Достоевского, e-mail: guts@omsu.ru.