

Даниленко А.И.

Институт проблем управления им. В.А. Трапезникова РАН

Информационное управление организационной системой с возможностью утечки информации

В наше время информация превратилась в важнейший стратегический ресурс общества. Сегодня практически для любой организации ключом к успеху является информация и грамотное ее использование. Зачастую эта информация ценна именно в силу неизвестности ее третьим лицам. Однако сам факт обладания информацией, как правило, не приносит ощутимого дохода; необходимо информацию разумно использовать, то есть должен быть определен круг лиц, имеющих доступ к этой информации. Исследования показывают, что причиной утечки информации в 70-80 процентах случаев служит намеренное разглашение конфиденциальной информации людьми, имеющими к ней санкционированный доступ в силу служебных обязанностей. Ключевым фактором представленной модели является возможность агентов делиться информацией друг с другом, что позволяет исследовать феномен утечки информации. Подобную возможность передачи информации удобно моделировать в терминах теории сетевых игр [1].

Рассмотрим организационную систему, состоящую из центра, множества $N = \{1, \dots, n\}$ его подчиненных (назовем их «своими» агентами) и множества $M = \{n + 1, \dots, n + m\}$ «чужих» агентов. На рис. 1 вершины графа, соответствующие своим агентам, изображены сплошными линиями, а вершины, обозначающие чужих агентов – пунктирными. Центр обладает некоторой информацией I_0 о существенных параметрах системы θ (будем называть совокупность этих параметров «состоянием природы») и, возможно, о представлениях других агентов о значении θ .

Примем следующий порядок функционирования системы. Центр, обладая правом первого хода, сообщает информацию I_0 подмножеству своих агентов $S_0 \subseteq N$, осуществляя, тем самым, *информационное управление* [2]. Таким образом формируется базовая *структура информированности* агентов. Далее реализуется сетевая игра: агенты, обладающие информацией, образуют направленные связи с другими агентами. Будем интерпретировать образование любой связи $ij; i, j \in N \cup M$ как *передачу*

информации. Утечкой информации будем называть передачу информации от своего агента чужому, то есть образование связи ij ; $i \in N, j \in M$. На рис. 1 утечка информации обозначена пунктирными дугами в графе.

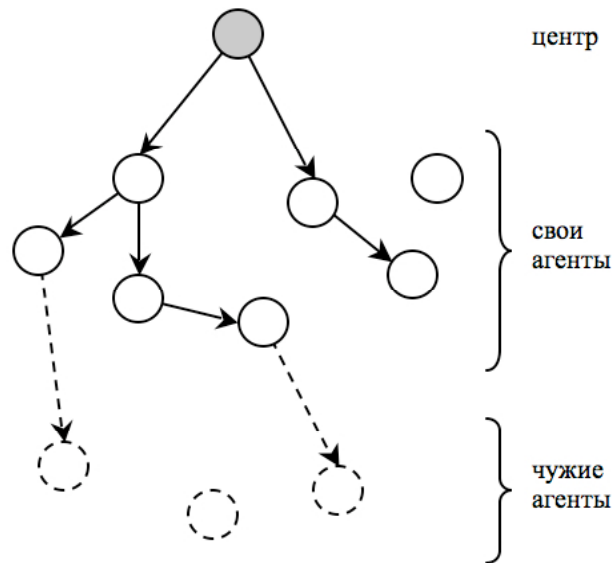


Рис. 1. Передача и утечка информации

Таким образом, действием i -го агента в разыгрываемой сетевой игре является подмножество агентов, которым он хочет передать полученную (от центра или от другого агента) информацию, то есть $x_i \subseteq N \cup M$. В итоге реализуется некоторая сеть g , однозначно определяющая множество агентов $S \subseteq N \cup M$, обладающих информацией. Множество информированных агентов S в совокупности с сообщением I_0 , которое является параметром модели, позволяет однозначно восстановить структуру информированности $I = I(S)$.

На последнем шаге агенты выбирают действия, не связанные с передачей информации, максимизируя свои целевые функции с учетом структуры информированности. При этом целевая функция центра зависит от состояния природы и от реализовавшегося множества информированных агентов:

$$F = F(\theta, S).$$

Последнее и определяет суть задачи информационной безопасности. Целевая функция центра такова, что он получает тем больше прибыль, чем больше своих и чем меньше чужих агентов обладают информацией. Формально это можно выразить следующими условиями:

$$\begin{aligned} \forall \theta, \forall S \subseteq N \cup M, \forall i \in N \setminus S : F(\theta, S) \leq F(\theta, S \cup \{i\}), \\ \forall \theta, \forall S \subseteq N \cup M, \forall j \in M \setminus S : F(\theta, S) \geq F(\theta, S \cup \{j\}). \end{aligned}$$

Таким образом, центр стремится передать информацию своим агентам, стараясь при этом избежать утечки. Стратегия центра в конкретной задаче определяется видом целевой функции. К примеру, в случае, когда любая утечка информации сводит прибыль центра к нулю, центр будет максимально осторожен и передаст информацию минимальному числу агентов, такой центр будем называть *принципиальным*. В случае если утечка информации не так сильно влияет на выигрыш центра, он может выбрать действие, которое приведет к небольшой утечке, но при этом будет способствовать широкому распространению информации среди своих агентов, что в итоге увеличит совокупную прибыль.

Стоит отметить, что в представленном виде постановка задачи является слишком общей, и ее решение является нецелесообразным. Однако описанная общая модель позволяет ставить и решать частные задачи в рамках очерченной проблематики. В частности, в рамках рассмотренной модели была сформулирована и подробно исследована задача защиты информации от утечки с двумя подчиненными, которые выполняют разные функции и имеют различные представления относительно неопределенного параметра – ценности (для центра) услуг, приобретаемых у стороннего контрагента. Исследование данной модели позволило сделать выводы относительно общих принципов поведения руководства и подчиненных в организационной системе с возможностью утечки информации.

СПИСОК ЛИТЕРАТУРЫ

1. Губко М.В. Управление организационными системами с сетевым взаимодействием агентов. Часть 1. Обзор теории сетевых игр. // Автоматика и телемеханика. – 2004. № 8.
2. Чхртишвили А.Г. Теоретико-игровые модели информационного управления. – М.: ПМСОФТ, 2004.