А. В. Лаврентьев, В. П. Зязин

О ПРИМЕНЕНИИ МЕТОДОВ ТЕОРИИ ИГР ДЛЯ РЕШЕНИЯ ЗАДАЧ КОМПЬЮТЕРНОЙ БЕЗОПАСНОСТИ

Развитие современных сетевых технологий сопровождается повышением требований к обеспечению приватности обработки информации и, как следствие, предполагает существенную модернизацию нормативно-методологической базы и стандартов управления информационной безопасностью. Между тем в этих документах отмечается, что в ряде случаев методы управления системами защиты информации, ориентированные на применение количественных оценок, все еще не имеют достаточно развитого математического аппарата для их обоснования. В работах последних лет прослеживается тенденция расширения имеющихся математических подходов к обоснованию параметров систем защиты за счет применения методов теории игр к решению задач обеспечения безопасности сетевых технологий, в том числе управления информационной безопасностью [1, 2, 3]. Применяемые теоретико-игровые подходы к решению задач информационной безопасности условно можно разделить на 2 класса: один класс (обозначим А) описывает взаимодействие «нападение — защита», предсказывая действия нападающих и определяя ответные действия защиты; второй (В) позволяет получать количественные оценки уровня защиты информационной системы путем предсказания действий нападающих и защиты.

В классе А можно выделить два подкласса игр — А1 и А2: игры подкласса А1 позволяют исследовать взаимодействие «нападение — защита» в общих случаях (игры обычно ведутся двумя игроками — «нападающим» и «защищающимся», и у каждого из них имеются всего по два возможных действия: {«нападать», «не осуществлять никаких действий»} и {«защищаться», «не осуществлять никаких действий»} соответственно); в подклассе А2 рассматриваются более сложные сценарии нападения и защиты, специализированные под конкретные ситуационные параметры (примером таких параметров могут быть свойства сети, в которой осуществляется взаимодействие). Игры подкласса А1 часто являются статическими играми с двумя игроками, или Байесовскими играми, которые хорошо исследованы в «классической» теории игр, и поэтому результаты игры относительно просто получить. Преимущества игр подкласса А2 в их большей реалистичности и лучшем описании динамики взаимодействия «нападающего» и «защищающегося», но получение выводов о «правильном» поведении участников требует значительных объемов вычислений, а решение в ряде случаев может не обладать достаточной точностью.

Многие подходы к оценке уровня информационной безопасности (например, риск-ориентированные, то есть применяющие понятие риска как метрику) используют в качестве входных данных предполагаемые стратегии нападающей и защищающейся сторон. Совмещение идей таких подходов с известными теоретико-игровыми методами привело к появлению класса В игр информационной безопасности, ориентированных на получение оценок и анализ уровня защищенности компьютерных систем. К этому классу, например, относится модель, описывающая, как инвестиции в обеспечение информационной безопасности одной организации могут влиять на безопасность других организаций. В терминах риска можно говорить о том, что такие инвестиции косвенно повышают безопасность других организаций в случае наличия общей сети у этих организаций или, наоборот, снижают чужую безопасность в силу снижения интереса злоумышленников к инвестирующей организации и последующего повышения его к другим организациям. Среди других моделей класса В представляет интерес более глубокое исследование кооперативной игры защищающихся организаций. В работе [4] найдены условия оптимальности формирования коалиций с целью противодействия злоумышленникам. Под оптимальностью здесь понимается условие, что любая пара уже сформированных коалиций имеет больше позитивных и меньше негативных

эффектов, чем в ситуации, когда они создадут одну общую коалицию. Взаимовлияние классов теоретико-игровых моделей информационной безопасности представлено на рис. 1.

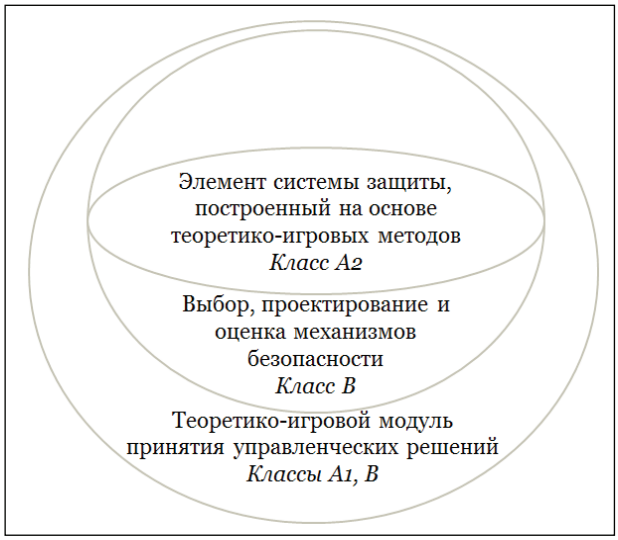

Рис. 1. Иерархия классов теоретико-игровых моделей информационной безопасности

Теоретико-игровые методы нашли широкое применение в задачах проектирования систем обнаружения вторжений (СОВ) [1, 5]. При этом вопросы противодействия атакам, направленным на саму СОВ, не получили должного исследования с позиции теории игр. В настоящее время к таким атакам относят [6]: сверхстимуляцию — создание большого количества паттернов, генерирующих ложные сигналы системы обнаружения вторжений, что приводит к перегрузке обработчиков событий; DoS-атаку на перегрузку сенсоров или замедление алгоритма, проверяющего паттерны.

В этой работе мы остановимся на узловых системах обнаружения вторжений (пример — BlueBoX [7]). Пусть Ω — множество наблюдаемых объектов, каждому из которых сопоставлено множество отслеживаемых параметров $I_{\omega\in\Omega}$.

Будем рассматривать следующее взаимодействие узловой СОВ и атакующего. Каждую атаку представим в виде некоторой последовательности шагов. Каждый шаг порождает некоторый вид активности, обнаруживаемый СОВ. После первой активности, которую СОВ распознала как подозрительную, осуществляется попытка предсказать последующие шаги предполагаемого злоумышленника и расширяется множество $I_{\omega\in\Omega}$ наблюдаемых параметров. Далее СОВ наблюдает расширенный список параметров в течение некоторого периода времени t_m. Обозначим $J_{\omega\in\Omega}$ множество дополнительных параметров наблюдения. До выявления подозрительной активности система обнаружения вторжений наблюдает базовый набор критических параметров. Очевидно, что в это время цена системных ресурсов постоянна. Обозначим $S(t)$ — цену дополнительных ресурсов, затрачиваемых на мониторинг множества $J_{\omega\in\Omega}$. Для простоты будем предполагать, что $S(t)$ линейно зависит от t, то есть

$$S(t) = \sum_{\omega\in\Omega} \sum_{j\in J_\omega} s(\omega, j, t) = fkt, \qquad (1)$$

где f — средний весовой коэффициент, определяющий цену одного наблюдаемого параметра, k — количество наблюдаемых пар «объект — параметр».

Для анализа стратегий СОВ и атакующего и оценки эффективности процесса мониторинга рассмотрим некооперативную теоретико-игровую модель с ненулевой суммой и несколькими итерациями. Количество итераций зависит от количества шагов атаки. Предполагается, что СОВ и атакующий взаимно знают стратегии и функции полезности друг друга. Когда СОВ обнаруживает подозрительную активность, она может решить проигнорировать ее или же усилить мониторинг.

В последнем случае количество наблюдаемых параметров будет увеличено. Время мониторинга для дополнительных параметров будет выбрано из информационной базы СОВ согласно сценарию атаки. Атакующий формирует свою стратегию на основе следующего множества действий: {«завершить атаку»; «продолжить без паузы»; «сделать паузу на некоторый период времени»}. Для иллюстрации игры будем использовать несколько типичных периодов подобных пауз.

В случае если узловая СОВ обнаруживает атаку или же злоумышленник решает прекратить нападение, выигрыш для системы обнаружения атаки будет α. В противном случае его значением будет $-\alpha$.

Атакующий может принадлежать одному из двух типов в зависимости от своих целей: проведение атаки на защищаемую систему или же на саму СОВ.

Первый тип атакующих получает выигрыш β в случае успешной атаки, иначе $-\beta$. Обозначим $Z(t)$ — стоимость паузы для атакующего, которую, так же как и в случае с СОВ, для простоты примем линейно зависящей от времени:

$$Z(t) = gt, \tag{2}$$

где g — весовой коэффициент, определяющий стоимость единичного периода паузы.

Таким образом, функция полезности для первого типа нападающих будет:

$$U_{at} = \begin{cases} 0, & NA, \\ \beta - R(t_a), & 0 \le t_m \le t_a, \\ -\beta - R(t_a), & t_m > t_a \ge 0, \end{cases} \tag{3}$$

где t_a — пауза между действиями нападающего, NA здесь и далее обозначает выбор злоумышленника завершить атаку.

Соответствующая первому типу атакующих функция полезности СОВ имеет вид

$$U^1_{mon} = \begin{cases} \alpha - R(t_m), & 0 \le t_a < t_m, NA, \\ -\alpha - R(t_m), & 0 \le t_m < t_a. \end{cases} \tag{4}$$

Для второго типа нападающих примем, что n — количество генерируемых нападающим паттернов. Так как предполагается, что с увеличением количества наблюдаемых объектов и времени их мониторинга, а также величины n вероятность определить тип нападающего возрастает, примем, что если n меньше некоторой величины, зависящей от t_m и k, то атака проходит успешно:

$$U_{ov} = \begin{cases} 0, & NA, \\ \beta + f(n+k)t_m, & n < F(t_m k), \\ -\beta, & n \ge F(t_m k). \end{cases} \tag{5}$$

Функция $F(t_m k) = \dfrac{N}{l^{t_m k}}$ будет использована для упрощения последующих вычислений, где N и l — числовые параметры, задаваемые начальным состоянием системы и особенностями реализации системы обнаружения вторжений. Соответствующая второму типу функция полезности СОВ:

$$U^2_{mon} = \begin{cases} \alpha - f(n+k)t_m, & n \ge F(t_m k), NA, \\ -\alpha - f(n+k)t_m, & n < F(t_m k). \end{cases} \tag{6}$$

Эта игра не может быть решена с использованием чистых стратегий, поэтому решение будет представлено в смешанных стратегиях. Ожидаемой выплатой для узловой СОВ будет

$$U_T = \sum_a \sum_b U_{mon}(a,b)\, p(a)\, p(b), \tag{7}$$

где $U_{mon}(a,b)$ — выплата СОВ, когда игроки выбирают стратегии a и b, а $p(a)$ и $q(b)$ — вероятности выбора этих стратегий СОВ и атакующим соответственно.

Для вычисления равновесия Нэша используем Gambit [8]. Далее рассмотрим пример того, как работает наша модель. СОВ будет осуществлять выбор на множестве из четырех действий: {a_1 = «игнорировать», a_2 = «увеличить количество наблюдаемых пар "объект — параметр" на 50, время мониторинга на 100 с», a_3 = «увеличить количество пар на 100, время мониторинга на 500 с», a_4 = «увеличить количество пар на 200, время мониторинга на 1500 с»}. Атакующий выбирает на множестве: {b_1 = «завершить нападение», b_2 = «продолжить атаку на защищаемый объект без паузы», b_3 = «сделать паузу на 400 с и продолжить атаку на защищаемый объект», b_4 = «сделать паузу на 1000 с и продолжить атаку на защищаемый объект», b_5 = «сформировать 10 паттернов для атаки на СОВ», b_6 = «сформировать 1000 паттернов для атаки на СОВ»}. Кроме того, примем $N = 2000, \alpha = 5000, \beta = 2000$ и $l = 1,0001$. В таблице 1 представлены результаты одного раунда. Таблицы 2 и 3 показывают стратегии игроков.

Таблица 1. Результаты первой итерации игры

	a_1	a_2	a_3	a_4
b_1	0; 5000	0; 4950	0; 4500	0; 2000
b_2	2000; -5000	-2000; 4950	-2000; 4500	-2000; 2000
b_3	1800; -5000	1800; -5050	-2200; 4500	-2200; 2000
b_4	1500; -5000	1500; -5050	1500; -5500	-2500; 2000
b_5	2000; -5000	2060; -5060	2550; -5550	-2000; 1985
b_6	2000; -5000	3050; -6050	-2000; 4450	-2000; 1985

Таблица 2. Стратегия атакующего

b_1	b_2	b_3	b_4	b_5	b_6	Ожидаемая полезность
0.6995816	0.02153313	0.0	0.0	0.2490239	0.02986128	0.0
0.6995493	0.0	0.0	0.0	0.2489484	0.05150225	0.0
0.6995799	0.02040104	0.0	0.0	0.2800189	0.0	0.0
0.6995493	0.0	0.0	0.0	0.3004506	0.0	0.0

Таблица 3. Стратегия СОВ

a_1	a_2	a_3	a_4	Ожидаемая полезность
0.5	0.0	0.0	0.5	1995.81672214
0.5	0.0	0.0	0.5	1995.49323986
0.5	0.0	0.0	0.5	1995.79971523
0.5	0.0	0.0	0.5	1995.49323986

В частности, из представленных таблиц видно, что в рассмотренном примере системе обнаружения вторжений следует выбирать с одинаковой вероятностью стратегии a_1 и a_4. В этом случае выплаты игроков будут 1995 и 0 для СОВ и атакующего соответственно.

В процессе тестирования модели была создана база знаний СОВ, состоящая из 10 сценариев атаки. Стратегии, основанные на ней, отличаются друг от друга как объектами и параметрами для мониторинга, так и значением t_m. Каждый сценарий был реализован 100 раз, и результаты отражают средние значения цены и процента обнаружения. Действия СОВ и атакующего выбирались согласно равновесию Нэша. Одновременно в целях сравнения для каждого сценария был подсчитан соответствующий объем ресурсов для традиционной реализации СОВ, обладающей 95-процентной точностью.

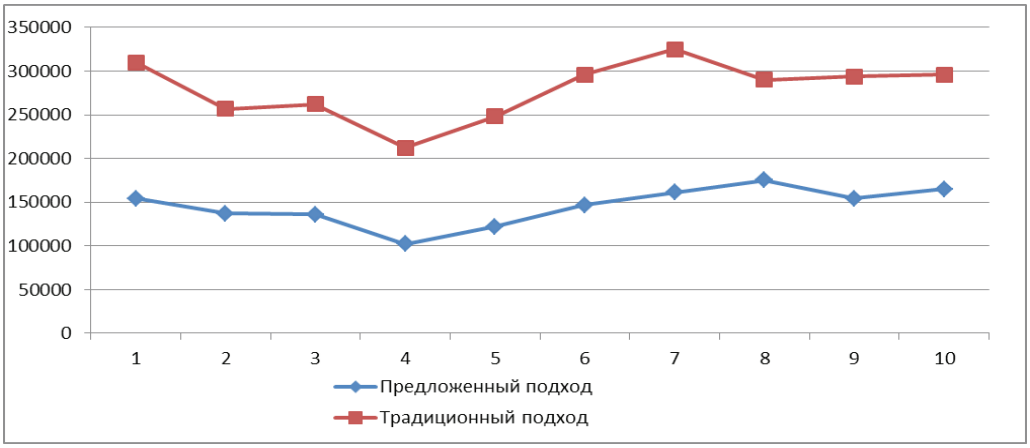

Рис. 2. Ценовое сравнение подходов

Рис. 3. Точность обнаружения предложенного подхода

Результаты представлены на рис. 2 и 3. Как можно заметить, количество необходимых ресурсов, требуемых для традиционной реализации, во много раз выше предложенного подхода. С другой стороны, точность обнаружения незначительно уступает нормальной реализации, но, тем не менее, оставляет возможным использование подобной теоретико-игровой оптимизации в системах с ограниченными ресурсами. В качестве дальнейшего исследования перспективным направлением была бы реализация возможности автоматического выбора времени мониторинга, например, с помощью введения в модель рефлексии [3].

СПИСОК ЛИТЕРАТУРЫ:

1. *Alpcan T., Başar T.* Network Security: A Decision and Game Theoretic Approach. Cambridge University Press, 2010.
2. *Зубов А. Ю.* Математика кодов аутентификации. М.: Гелиос АРВ, 2007.

3. *Губанов Д. А., Новиков Д. А., Чхартишвили А. Г.* Социальные сети: модели информационного влияния, управления и противоборства. М.: Физматлит, 2010.
4. *Saad W., Alpcan T., Başar T., Hjurungnes A.* Coalitional game theory for security risk management // In Proceedings of the 5th International Conference on Internet Monitoring and Protection (ICIMP '10). Washington, DC, USA. May 2010. P. 35—40.
5. *Manshaei M. H., Zhu Q., Alpcan T., Başar T., Hubaux J.-P.* Game Theory Meets Network Security and Privacy // ACM Computing Surveys. 2013. 45. No 3:25.
6. *Corona I., Giacinto G., Roli F.* Adversarial attacks against intrusion detection systems: Taxonomy, solutions and open issues // Information Sciences. 2013. Vol. 239. P. 201—225.
7. *Chari S. N., Cheng P.-C.* BlueBoX: A policy-driven, host-based intrusion detection system // ACM Transaction on Information and System Security. May 2003. Vol. 6. No. 2. P. 173—200.
8. *McKelvey R. D., McLennan A. M., Turocy T. L.* Gambit: Software Tools for Game Theory, Version 13.1.0. http://www.gambit-project.org (accessed 01.10.13).