DOI 10.37882/2223-2966.2024.01.33

ПРИМЕНЕНИЕ ТЕОРИИ КООПЕРАТИВНЫХ ИГР ДЛЯ ОЦЕНКИ БЕЗОПАСНОСТИ СИСТЕМЫ

APPLICATION OF COOPERATIVE GAME THEORY TO ASSESS SYSTEM SECURITY

L. Stepanov
A. Salnikova

Summary. System security issues are one of the priorities. To solve it, various measures can be applied that partially or completely neutralize the negative impact (destructive activity) on the system. The publication proposes to apply the theory of cooperative games and the Shapley vector to find the optimal combination of security measures and in relation to destructive activities. The publication examines the main issues of security and introduces the concept of destructive activity, as it summarizes the various types and sources of negative impact on the security of the system. Due to the fact that the neutralization of destructive activity cannot be carried out using only one event, it justifies the application of the theory of cooperative games and the Shapley vector to determine the optimal coalition of activities. A numerical example of the application of the Shapley vector to the problem of safety assessment is considered.

Keywords: system, security, threat, destructive activity, security measures, attacker, theories of cooperative games, Shapley vector.

Степанов Леонид Викторович
Доктор технических наук, профессор, доцент, Федеральное казенное образовательное учреждение высшего образования Воронежский институт ФСИН России, Воронеж
StepanovLV@yandex.ru
Сальникова Анастасия Юрьевна
Адъюнкт, Федеральное казенное образовательное учреждение высшего образования Воронежский институт ФСИН России, Воронеж
salnikova.nastya1999@yandex.ru

Аннотация. Вопросы безопасности систем являются одной из приоритетных задач. Для ее решения могут применяться различные мероприятия, которые частично или полностью нейтрализуют отрицательное влияние (деструктивную деятельность) на систему. В публикации предлагается применить теорию кооперативных игр и вектор Шепли для нахождения оптимального сочетания мероприятий по обеспечению безопасности и по отношению к деструктивной деятельности. В публикации рассмотрены основные вопросы обеспечения безопасности и введено понятие деструктивной деятельности, так как оно обобщает различные виды и источники негативного влияния на безопасность системы. В силу того, что нейтрализация деструктивной деятельности не может быть осуществлена с использованием только одного мероприятия, обосновывает применение теории кооперативных игр и вектора Шепли для определения оптимальной коалиции мероприятий. Рассмотрен числовой пример применения вектора Шепли к задаче оценки безопасности.

Ключевые слова: система, безопасность, угроза, деструктивная деятельность, мероприятия по обеспечению безопасности, злоумышленник, теории кооперативных игр, вектор Шепли.

Безопасность является комплексным понятием, которое требует разнообразных мероприятий и воздействий для защиты от угроз и обеспечения безопасности в различных областях деятельности и ситуациях. Эффективные мероприятия по обеспечению безопасности могут включать комбинацию технических, организационных и правовых мер, а также обучение персонала и постоянное обновление систем безопасности в соответствии с развивающимися угрозами. В современных условиях проблема выявления и нейтрализации деструктивной деятельности является приоритетной задачей.

Например, безопасность в сетях ЭВМ является важной составляющей, особенно во время цифровых технологий. Мероприятия по обеспечению безопасности в сети включают в себя защиту сетей и систем от хакерских атак, вирусов и вредоносного программного обеспечения с помощью различных технических средств, и программ. Для получения доступа к передаваемой по каналам связи информации, проводится мониторинг каналов системы электросвязи, относящийся к пассивным или нейтральным видам деятельности в информационном пространстве [1].

Целью данной публикации является анализ возможности применения теории кооперативных игр и, в частности, вектора Шепли для нахождения сочетания мероприятий по обеспечению безопасности (МпОБ) для противодействия деструктивной деятельности (ДД).

Введем понятие деструктивная деятельность (ДД) — планируемое и (или) практически реализуемое воздействие на уровень безопасности системы (охраняемы объект) с целью понижения этого уровня и (или) создания условий для такого понижения [2].

Источником ДД могут быть внешние и внутренние по отношению к системе злоумышленники или неумыш-

ленные действия (или бездействие) персонала. ДД злоумышленников может привести к различным неблагоприятным последствиям для охраняемого объекта. Она включает в себя угрозы физических повреждений людей, ущерб материальных ценностей, насилие, контрабанду запрещенных предметов и наркотиков, а также другие формы правонарушений. В связи с тем, что ДД может носить непреднамеренный характер, ее источником может быть персонал предприятия (организации, фирмы, учреждения). Данная категория ДД включает в себя такие непреднамеренные действия, как ошибки в работе или недобросовестное выполнение служебных обязанностей. Такие ДД могут привести к нарушению безопасности объекта, утечке конфиденциальной информации или несанкционированному доступу к системам. Для предотвращения этих последствий необходимо регулярно проводить обучение персонала, усиливать контроль над доступом к информации и применять технические средства защиты. Важно также разрабатывать и регулярно обновлять политику безопасности организации, чтобы персонал был осведомлен о возможных опасностях и знал, как справиться с ними.

К ним относятся, в первую очередь, организационно-правовые меры, такие как разработка и применение нормативных актов, регулирующих порядок деятельности в рассматриваемой системе. Кроме организационно-правовых мер, для нейтрализации ДД могут применяться программные и инженерно-технические мероприятия. К ним относят, разработку и применение специализированного программного обеспечения, которая позволяет производить контроль и управление системой безопасности, а также автоматизировать процессы обнаружения и реагирования на возможные нарушения. Инженерно-технические мероприятия, в свою очередь, включают в себя применение специального оборудования, систем видеонаблюдения, контроля доступа и других технических средств, которые способствуют выявлению и предотвращению угроз безопасности.

Сочетание различных мероприятий по обеспечению безопасности позволяет создать комплексную систему защиты, которая обеспечит надежную защиту объекта и его сотрудников от возможных угроз и рисков. Однако, важно отметить, что эффективность такой системы будет зависеть от правильного выбора и применения мер, а также от оценки и учета специфики конкретного объекта и его потенциальных уязвимостей [2].

Теория Шепли имеет глубокие математические основы и не требует обширных вычислительных ресурсов для проведения точных расчетов. В целом, эта теория позволяет объективно определить разделение выигрышей в коалиционных играх и способствует достижению более справедливых и эффективных результатов [3].

Метод Шепли активно используется в экономике для определения структуры распределения прибыли между участниками компаний или владельцами акций. Кроме того, метод Шепли находит применение в политологии при определении влияния различных партий или групп интересов в политических системах. Также метод Шепли имеет широкое применение в логистике и транспортировке, когда необходимо распределить грузы между различными транспортными средствами или маршрутами с учетом вклада каждого транспортного узла. Он также может быть использован для анализа коалиционных игр и принятия справедливых долей при решении международных конфликтов или проблем разделения территории.

Таким образом, метод Шепли является мощным инструментом для решения задач, требующих справедливого распределения ресурсов и учета вклада каждого участника [4, 5]. Его применение позволяет достичь сбалансированных и устойчивых решений в самых различных ситуациях. Кроме того, актуальность исследования метода Шепли состоит в том, что в открытой печати недостаточно встречается его применений в сферах обеспечения безопасности.

Так как понятие безопасности носит системный характер (ДД и МпОБ формируют систему), введем следующую формализацию МпОБ и ДД:

$$\begin{aligned} M &= \{m_1; m_2; m_3; \ldots; m_i; \ldots m_n\}, \\ DD &= \{d_1; d_2; d_3; \ldots; d_j; \ldots; d_k\} \end{aligned} \quad (1)$$

где m_i — i-тое МпОБ; $i = \overline{1,n}$; n — количество МпОБ, d_j — j-тое ДД; $j = \overline{1,k}$; k — количество деструктивных воздействий.

Каждое МпОБ представляет собой совокупность практических действий (ПД) по обеспечению безопасности:

$$m_i = \{p_{i1}; p_{i2}; p_{i3}; \ldots; p_{if}; \ldots; p_{it_i}\} \quad (2)$$

где $f = \overline{1,t_i}$ t_i — количество практических действий для i-того МпОБ.

Таким образом в графической форме МпОБ можно представить в виде (см. рисунок 1).

Следовательно, нужно найти такое сочетание МпОБ из (1) для каждого ДД из DD, чтобы обеспечивалась максимизация эффективности нейтрализации ДД. Для этой цели предлагается использовать вектор Шепли [3, 6]:

$$X_i(V) = \sum_{S \ni i} \frac{(|S|-1)!(n-|S|)!}{n!} \left(V(S) - V(S \setminus \{i\})\right), \quad (3)$$

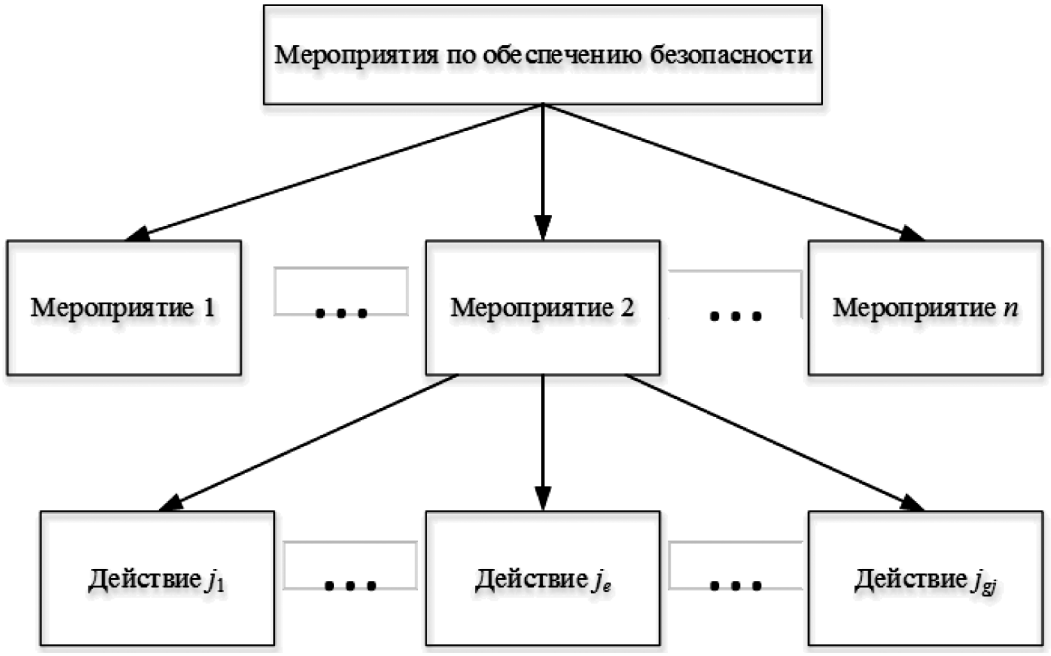

Рис. 1. Мероприятия по обеспечению безопасности

где $i = 1,2…n$; X — дележ; S — количество игроков; n — количество участников дележа.

Основные результаты

Рассмотрим возможность достижения поставленной цели на примере. Пусть есть некоторая ДД, негативно влияющая на режим безопасности системы и есть три МпОБ, которые могут нейтрализовать данную ДД и формируются на основе пяти ПД:

$$M = \{m_1; m_2; m_3\}, m_i = \{p_{i1}; p_{i2}; p_{i3}; p_{i4}; p_{i5}\}. \quad (4)$$

Каждое из МпОБ состоит из определенных ПД, эффективность которых экспертно оценена в диапазоне от 0 до 100 (см. таблицу 1).

Таблица 1.

Экспертная оценка эффективности ПД по отношению к ДД

Практическое действие	p_1	p_2	p_3	p_4	p_5	Суммарная эффективность
Экспертная оценка	15	25	15	10	20	85

Следует обратить внимание, что ни одно отдельное ПД не имеет высокой эффективностью по отношению ДД и суммарная эффективность менее 100. Таким образом, возникает необходимость поиска сочетания МпОБ из (4).

В реальных условиях может возникать вопрос целесообразности реализации повторяющихся действий в составе различных МпОБ, а также рассмотрим случай синергетического эффекта ПД в коалициях МпОБ. Будем полагать, что синергетический эффект равен 10 при $\{p_1; p_2\}$, $\{p_1; p_3\}$ и $\{p_3; p_4\}$.

Тогда для множества МпОБ (4) получим оценки эффективности, представленные в таблице 2. Здесь m_2 и m_3 получают синергию, так как содержат действия $\{p_1; p_3\}$ и $\{p_1; p_2\}$ соответственно.

Таблица 2.

Оценка эффективности МпОБ по отношению к ДД в случае не повторяемости ПД и синергетического эффекта

	p_1	p_2	p_3	p_4	p_5	Эффективность МпОБ
m_1	15	0	0	10	20	45
m_2	15	0	15	0	20	60
m_3	15	25	0	10	20	80

Следует отметить, суммарная оценка эффективности МпОБ может быть более 100, что будет указывать на избыточность МпОБ к ДД.

В соответствии с теорией кооперативных игр могут быть сформированы коалиции, для каждой из которых значение характеристической функции предлагается определить арифметическим суммированием оценок эффективности ПД и эффективностей МпОБ (см. таблицу 3). Однако, для этой цели могут быть применены и другие способы вычисления V.

Тогда, на основе таблицы 3 могут быть определены значения компонентов вектора Шепли:

Таблица 3.

Характеристическая функция вектора Шепли

	$\{m_1\}$	$\{m_2\}$	$\{m_3\}$	$\{m_1;m_2\}$	$\{m_2;m_3\}$	$\{m_1;m_3\}$	$\{m_1;m_2;m_3\}$
V	45	60	80	105	140	125	185

1. для коалиции: $\{m_1;m_2;m_3\}$:

$$X_1 = \frac{(1-1)!(3-1)!}{3!}(45-0) + \frac{(2-1)!(3-2)!}{3!}(105-60) + \frac{(2-1)!(3-2)!}{3!}(125-80) + \frac{(3-1)!(3-3)!}{3!}(185-140) = 45$$

$$X_2 = \frac{(1-1)!(3-1)!}{3!}(60-0) + \frac{(2-1)!(3-2)!}{3!}(105-45) + \frac{(2-1)!(3-2)!}{3!}(140-80) + \frac{(3-1)!(3-3)!}{3!}(185-125) = 60$$

$$X_3 = \frac{(1-1)!(3-1)!}{3!}(80-0) + \frac{(2-1)!(3-2)!}{3!}(125-45) + \frac{(2-1)!(3-2)!}{3!}(140-60) + \frac{(3-1)!(3-3)!}{3!}(185-105) = 79,98$$

2. для коалиции: $\{m_1;m_2\}$:

$$X_1 = \frac{(1-1)!(2-1)!}{2!}(45-0) + \frac{(2-1)!(2-2)!}{2!}(105-60) = 45$$

$$X_2 = \frac{(1-1)!(2-1)!}{2!}(60-0) + \frac{(2-1)!(2-2)!}{2!}(105-45) = 60$$

3. для коалиции: $\{m_2;m_3\}$:

$$X_2 = \frac{(1-1)!(2-1)!}{2!}(60-0) + \frac{(2-1)!(2-2)!}{2!}(140-80) = 60$$

$$X_3 = \frac{(1-1)!(2-1)!}{2!}(80-0) + \frac{(2-1)!(2-2)!}{2!}(140-60) = 80$$

4. для коалиции: $\{m_1;m_3\}$:

$$X_1 = \frac{(1-1)!(2-1)!}{2!}(45-0) + \frac{(2-1)!(2-2)!}{2!}(125-80) = 45$$

$$X_3 = \frac{(1-1)!(2-1)!}{2!}(80-0) + \frac{(2-1)!(2-2)!}{2!}(125-45) = 80$$

Так как по постановке задачи требуется максимизировать эффективность МпОБ, для выбора коалиции предлагается использовать условие:

$$X_{S(i)} > X_i(V), \quad (5)$$

а эффективность коалиции определить, как:

$$E_s = \sum_{i=1}^{|S|} X_i \quad (6)$$

В силу тог, что теория кооперативных игр отличается высокой гибкостью, в качестве дополнительного условия выбора коалиции введем трудозатратность реализации всех ПД (см. таблицу 4).

Таблица 4.

Суммарное значение эффективности для коалиций

	$m_1; m_2$	$m_2; m_3$	$m_1; m_3$	$m_1; m_2; m_3$
Эффективность коалиций	105	140	125	184,98
Практические действия	$p_1; p_3; p_4; p_5$	$p_1; p_2; p_3; p_4; p_5$	$p_1; p_2; p_4; p_5$	$p_1; p_2; p_3; p_4; p_5$

Исходя из исходных ограничений необходимо выбрать коалицию: $\{m_1;m_3.\}$. Она имеет максимальное значение E_s и не предполагает выполнения всех ПД. Аналогично можно определить сочетание МпОБ для всех ДД.

Заключение

Теория кооперативных игр и вектор Шепли могут быть использованы для оценки уровня безопасности системы, а их возможности позволяют:

1. не только для определить справедливый дележ между участниками коалиции, но и выбрать оптимальную;
2. учесть различные условия формирования коалиций (повторяемость или не повторяемость ПД);
3. использовать разнообразные варианты расчета значений характеристической функции для ПД и МпОБ, а также учесть специфические условий формирования коалиций;

4. учесть различные критерии поиска оптимальной коалиции (максимизация эффективности МпОБ, трудозатратность ПД, минимизация избыточности МпОБ по отношению к ДД).

ЛИТЕРАТУРА

1. Баранова, Е.К. Информационная безопасность и защита информации: учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва: РИОР: ИНФРА-М, 2022. — 336 с.
2. Степанов Л.В. Подход к выявлению деструктивной деятельности в учреждениях пенитенциарной системы / Степанов Л.В., Сальникова А.Ю. // Математические методы и информационные технологии в моделировании систем: материалы VII Всероссийской (национальной) научно-практической конференции [Текст] / редкол.: Н.В. Боковая [и др.]; Воронежский филиал РЭУ имени Г. В. Плеханова. Воронеж: Издательство «Научная книга», 2023. — С. 68–73
3. Наумова, Н.И. Вектор Шепли и его обобщения: Учебное пособие / Н.И. Наумова. — Санкт-Петербург: ООО «Издательство ВВМ», 2017. — 60 с.
4. Сигал, А.В. Теория игр и ее экономические приложения: учебное пособие / А.В. Сигал. — Москва: ИНФРА-М, 2024. — 418 с.
5. Степанов Л.В. Практические аспекты применения теории игр к оценке безопасности системы / Л.В. Степанов, А.С. Кольцов, А.В. Паринов, Д.В. Паринов, Б.А. Соловьев // Моделирование, оптимизация и информационные технологии, № 4(27), 2019. — С.46–47
6. Теория игр. Примеры и задачи: учебное пособие / В.П. Невежин. — Москва: ФОРУМ: ИНФРА-М, 2024. — 128 с.

© Степанов Леонид Викторович (StepanovLV@yandex.ru); Сальникова Анастасия Юрьевна (salnikova.nastya1999@yandex.ru)
Журнал «Современная наука: актуальные проблемы теории и практики»