DOI 10.37882/2223-2966.2024.06.06

МАТЕМАТИЧЕСКОЕ МОДЕЛИРОВАНИЕ ЗАДАЧ ИНФОРМАЦИОННОЙ ЗАЩИТЫ С ПОМОЩЬЮ ТЕОРИИ ИГР

MATHEMATICAL MODELING OF INFORMATION SECURITY TASKS USING GAME THEORY

B. Bondarenko

Summary. The article discusses the application of game theory methods for modeling and analysis of information security tasks. The rationale for using game-theoretic models to account for rational behavior of opponents, optimal allocation of defense resources, and selection of the most effective countermeasure strategies is provided. Examples of constructing game models for various attack and defense scenarios are given, and approaches to improving the effectiveness of security systems based on the obtained results are proposed. The necessity of a comprehensive approach combining the application of game theory with other information security methods and tools is emphasized.

Keywords: information security, game theory, threat modeling, optimal defense strategies, resource allocation, rational behavior of opponents.

Бондаренко Богдан Павлович
Волгоградский Государственный Технический Университет
bogdanbondarenko19@yandex.ru

Аннотация. В статье рассматривается применение методов теории игр для моделирования и анализа задач информационной безопасности. Обосновывается целесообразность использования теоретико-игровых моделей для учета рационального поведения противников, оптимального распределения ресурсов защиты и выбора наиболее эффективных стратегий противодействия угрозам. Приводятся примеры построения игровых моделей для различных сценариев атак и защиты, а также предлагаются подходы к повышению эффективности систем безопасности на основе полученных результатов. Подчеркивается необходимость комплексного подхода, сочетающего применение теории игр с другими методами и средствами информационной защиты.

Ключевые слова: информационная безопасность, теория игр, моделирование угроз, оптимальные стратегии защиты, распределение ресурсов, рациональное поведение противников.

В эпоху цифровой трансформации и глобализации информационных систем обеспечение информационной безопасности приобретает критическую важность. Злоумышленники, стремящиеся получить несанкционированный доступ к конфиденциальным данным или нарушить целостность и доступность информационных ресурсов, представляют серьезную угрозу для организаций во всех сферах деятельности. Защита от таких угроз требует комплексного подхода, учитывающего не только технические аспекты, но и поведение рациональных противников, стремящихся максимизировать свою выгоду. В этом контексте теория игр предлагает мощный математический аппарат для моделирования и анализа конфликтных ситуаций в области информационной безопасности. Применение теоретико-игровых моделей позволяет формализовать взаимодействие сторон, определить их оптимальные стратегии и найти равновесные решения, обеспечивающие наиболее эффективное распределение ограниченных ресурсов защиты.

Задачи обеспечения информационной безопасности по своей природе представляют собой антагонистические конфликтные ситуации, в которых интересы сторон противоположны. С одной стороны, есть субъекты, стремящиеся получить несанкционированный доступ к информационным ресурсам или нарушить их целостность и доступность. С другой стороны, существуют субъекты, ответственные за защиту информации и предотвращение таких угроз [1, 2]. Данная ситуация характеризуется наличием рационально действующих противников с противоположными целями, что делает ее идеальным объектом для применения методов теории игр.

Теория игр представляет собой математический инструментарий для анализа конфликтных ситуаций, в которых участники преследуют противоположные интересы [3]. Она позволяет формализовать взаимодействие сторон, определить их оптимальные стратегии и найти равновесные решения. В контексте информационной безопасности, теория игр может быть использована для моделирования и анализа угроз, а также выбора наиболее эффективных средств и методов защиты [4, 5]. Одним из ключевых преимуществ применения теории игр в задачах информационной защиты является возможность учета рационального поведения противника [6]. Злоумышленники, как правило, действуют целенаправленно и стремятся максимизировать свою выгоду, выбирая наиболее эффективные методы атаки. Теория игр позволяет предсказать их потенциальные действия и разработать соответствующие контрмеры [7]. Кроме того, теория игр предоставляет инструменты для оптимального распределения ограниченных ресурсов, выделяемых на обеспечение информационной безопасности [8]. Это особенно актуально, поскольку средства защиты могут быть дорогостоящими, а их внедрение сопряжено с определенными издержками и рисками [9, 10]. При-

менение методов теории игр в задачах информационной защиты позволяет учитывать множество факторов, таких как вероятности различных угроз, эффективность средств защиты, затраты на их внедрение и потенциальный ущерб от реализации угроз [11, 12]. На основе этих данных строятся математические модели, которые используются для выбора оптимальных стратегий защиты и распределения ресурсов [13].

Следует отметить, что существует множество различных подходов к применению теории игр в задачах информационной безопасности, включая игры с полной и неполной информацией, статические и динамические игры, игры с нулевой суммой и игры с ненулевой суммой [14, 15]. Выбор конкретного подхода зависит от специфики рассматриваемой задачи и имеющихся данных. Таким образом, задачи информационной защиты по своей природе представляют собой антагонистические конфликтные ситуации, в которых методы теории игр являются эффективным инструментом для анализа, моделирования и принятия решений. Применение теории игр позволяет учитывать рациональное поведение противника, оптимально распределять ресурсы и выбирать наиболее эффективные стратегии защиты [16, 17].

Для применения теории игр к задачам информационной защиты необходимо адаптировать ее основные элементы к специфике рассматриваемой области. Прежде всего, следует определить участников игры, или игроков. В контексте информационной безопасности игроками являются субъекты, стремящиеся получить несанкционированный доступ к информационным ресурсам (злоумышленники, хакеры), и субъекты, ответственные за защиту этих ресурсов (администраторы безопасности, специалисты по информационной защите). Далее необходимо сформулировать множества стратегий игроков. Стратегией злоумышленника может быть выбор определенного метода атаки (например, эксплуатация уязвимостей, социальная инженерия, распределенная атака типа «отказ в обслуживании» и т.д.) [8, 13]. Стратегией защитника, в свою очередь, является выбор конкретных средств и механизмов защиты (антивирусные программы, межсетевые экраны, системы обнаружения вторжений, политики безопасности и т.п.) [9, 10]. Следующим шагом является определение функций выигрыша или проигрыша для каждого игрока. Эти функции должны отражать ценность различных исходов игры для участников. Для злоумышленника функция выигрыша может быть связана с ценностью получаемой информации, потенциальным ущербом от реализации атаки или вероятностью успешного проникновения [12]. Для защитника функция проигрыша, как правило, определяется вероятностью реализации угроз, потенциальным ущербом от них и затратами на внедрение средств защиты [7, 11]. После формализации основных элементов игры можно переходить к построению теоретико-игровых моделей. Выбор конкретного типа модели (игра с полной или неполной информацией, статическая или динамическая игра, игра с нулевой или ненулевой суммой) зависит от специфики рассматриваемой задачи и имеющихся данных [14, 15].

Важной особенностью задач информационной защиты является наличие множества различных угроз и средств защиты, что приводит к необходимости построения многокомпонентных или многоэтапных игровых моделей. В таких моделях отдельные игры могут соответствовать различным типам угроз или этапам процесса защиты (предотвращение, обнаружение, реагирование) [16, 17]. Кроме того, в задачах информационной безопасности часто присутствует элемент неопределенности и недостатка информации. Злоумышленники могут скрывать свои истинные намерения и возможности, а защитники не всегда могут точно оценить эффективность применяемых средств защиты. В таких случаях могут использоваться игры с неполной информацией, байесовские игры или стохастические игровые модели [18, 19]. Следует также отметить, что в реальных ситуациях информационной защиты зачастую присутствуют множественные игроки с различными интересами и ролями. Например, помимо злоумышленников и защитников, могут быть вовлечены сторонние наблюдатели, разработчики средств защиты, регулирующие органы и т.д. Для моделирования таких ситуаций могут применяться игры с несколькими участниками или иерархические игровые модели [20, 21].

Таким образом, адаптация теоретико-игровых моделей к задачам информационной защиты требует тщательного анализа специфики рассматриваемой ситуации, определения участников игры, их стратегий и функций выигрыша/проигрыша. Необходимо учитывать многокомпонентный характер задач информационной безопасности, элементы неопределенности и наличие множественных игроков с различными интересами. Построение адекватных игровых моделей позволяет глубже понять природу конфликта в области информационной защиты и найти оптимальные стратегии противодействия угрозам.

Рассмотрим конкретные примеры применения теоретико-игровых моделей для анализа угроз информационной безопасности и выбора оптимальных стратегий защиты. Также проанализируем различные подходы к повышению эффективности систем защиты на основе полученных результатов.

Пример 1. Игра с нулевой суммой для моделирования атаки на веб-сервер.

Рассмотрим ситуацию, в которой злоумышленник пытается получить несанкционированный доступ к веб-

серверу организации с целью кражи конфиденциальных данных. Предположим, что злоумышленник может использовать одну из следующих стратегий атаки:

- Атака с применением эксплойтов (A1)
- Атака с использованием вредоносного ПО (A2)
- Атака типа «отказ в обслуживании» (A3)

Защитник, в свою очередь, может выбрать одну из следующих стратегий защиты:

- Установка межсетевого экрана (D1)
- Внедрение системы обнаружения вторжений (D2)
- Использование антивирусного ПО (D3)

Матрица выигрышей для этой игры с нулевой суммой может выглядеть следующим образом (Рисунок 1):

	D1	D2	D3
A1	0.3, -0.3	0.7, -0.7	0.6, -0.6
A2	0.5, -0.5	0.3, -0.3	0.1, -0.1
A3	0.2, -0.2	0.4, -0.4	0.8, -0.8

Рис. 1. Матрица выигрышей

В этой матрице элементы представляют собой пары (x, y), где x — выигрыш злоумышленника, а y — выигрыш защитника. Так как это игра с нулевой суммой, выигрыш одного игрока равен проигрышу другого ($x + y = 0$).

Используя различные методы решения игр (например, метод Брауна-Робинсона), можно найти оптимальные смешанные стратегии для обоих игроков. Пусть оптимальные стратегии будут следующими:

- Злоумышленник: (0.4, 0.3, 0.3)
- Защитник: (0.2, 0.6, 0.2)

Это означает, что злоумышленнику следует со следующими вероятностями применять различные стратегии атаки: A1 — 0.4, A2 — 0.3, A3 — 0.3. Защитнику, в свою очередь, рекомендуется со следующими вероятностями использовать средства защиты: D1 — 0.2, D2 — 0.6, D3 — 0.2.

При использовании оптимальных смешанных стратегий ожидаемый выигрыш злоумышленника составит 0.42, а ожидаемый проигрыш защитника — (-0.42). Это означает, что при данном распределении ресурсов вероятность успешной атаки составляет 0.42.

Чтобы повысить эффективность системы защиты, защитник может предпринять следующие шаги:

1. Увеличить бюджет на средства защиты и внедрить дополнительные механизмы безопасности.
2. Провести более глубокий анализ угроз и уязвимостей для выявления слабых мест в существующей системе защиты.
3. Разработать комплексную стратегию безопасности, включающую в себя не только технические средства защиты, но и организационные меры и обучение персонала.
4. Рассмотреть возможность использования ложных информационных ресурсов для отвлечения злоумышленников и сбора данных об их тактике.

Пример 2. Байесовская игра для моделирования атаки на базу данных.

В этом примере рассматривается ситуация, когда злоумышленник пытается получить доступ к базе данных организации, содержащей конфиденциальную информацию. Однако защитник не располагает полной информацией о типе и целях атаки, поэтому для моделирования этой ситуации используется байесовская игра.

Предположим, что злоумышленник может выбрать одну из двух стратегий:

- Атака с использованием эксплойтов (A1)
- Атака с применением методов социальной инженерии (A2)

Защитник, в свою очередь, может выбрать одну из следующих стратегий защиты:

- Установка системы обнаружения вторжений (D1)
- Усиление политик безопасности и обучение персонала (D2)

Матрица выигрышей для данной игры имеет следующий вид:

	D1	D2
A1	-2, 2	5, -5
A2	4, -4	-1, 1

Рис. 2. Матрица выигрышей

Защитник считает, что с вероятностью 0.6 злоумышленник выберет стратегию A1, и с вероятностью 0.4 — стратегию A2. Эти вероятности представляют априорные убеждения защитника относительно намерений злоумышленника.

Используя методы решения байесовских игр, можно найти оптимальные стратегии для обоих игроков. Пусть оптимальные стратегии будут следующими:

- Злоумышленник: (0.8, 0.2)
- Защитник: (0.4, 0.6)

Это означает, что злоумышленнику рекомендуется с вероятностью 0.8 использовать стратегию A1 (атака с эксплойтами) и с вероятностью 0.2 — стратегию A2 (социальная инженерия). Защитнику следует с вероятностью 0.4 применять стратегию D1 (система обнаружения вторжений) и с вероятностью 0.6 — стратегию D2 (усиление политик безопасности и обучение персонала).

При использовании оптимальных стратегий ожидаемый выигрыш злоумышленника составит 1.6, а ожидаемый проигрыш защитника — (-1.6). Это означает, что при данном распределении ресурсов вероятность успешной атаки составляет 0.4.

Для повышения эффективности системы защиты в этом случае защитник может предпринять следующие шаги:

1. Провести более глубокий анализ угроз и пересмотреть априорные вероятности выбора стратегий злоумышленником. Возможно, имеющаяся информация является недостаточно точной или устаревшей.
2. Инвестировать в развитие программ обучения и повышения осведомленности персонала в вопросах информационной безопасности. Это позволит снизить риски, связанные с атаками на основе социальной инженерии.
3. Рассмотреть возможность внедрения дополнительных средств защиты, таких как системы предотвращения вторжений (IPS), средства контроля доступа, шифрования данных и т.д.
4. Усилить меры по мониторингу и аудиту системы безопасности, чтобы своевременно выявлять попытки несанкционированного доступа и принимать соответствующие контрмеры.
5. Разработать комплексную стратегию реагирования на инциденты информационной безопасности, включающую в себя процедуры выявления, анализа, сдерживания и ликвидации последствий атак.
6. Рассмотреть возможность использования методов активной защиты, таких как ложные информационные ресурсы (honeypot) и обманные системы (deception systems), для сбора данных о тактике злоумышленников и отвлечения их от реальных ценных активов.
7. Регулярно проводить тестирование на проникновение (пентесты) для выявления потенциальных уязвимостей и оценки эффективности существующих средств защиты.
8. Наладить сотрудничество и обмен информацией об угрозах с другими организациями и специализированными центрами по кибербезопасности для получения актуальных данных о новых видах атак и методах защиты.

Понимание глубинной взаимосвязи между обеспечением эффективной защиты информационных систем и многогранным, целостным подходом, простирающимся далеко за пределы технических средств защиты, является фундаментальным для успешной реализации стратегии информационной безопасности. Создание комплексной стратегии требует всеобъемлющего осмысления, синтезирующего организационные меры, непрерывный процесс обучения персонала, тщательный и непрерывный мониторинг и постоянное совершенствование процессов обеспечения безопасности, органично переплетенных с технической составляющей.

Теоретико-игровые модели, основанные на строгом математическом аппарате и глубоком теоретическом фундаменте, предоставляют ценную аналитическую информацию, проливающую свет на анализ угроз, оценку рисков и оптимальное распределение ограниченных ресурсов защиты, являющихся неотъемлемой частью любой стратегии информационной безопасности [14]. Тем не менее, результаты, полученные путем применения этих моделей, требуют тщательного аналитического осмысления, интегрирующего их в общую стратегию информационной безопасности организации, основанную на глубоком понимании ее специфики, целей и задач, обеспечивая синергию теоретических и прикладных аспектов защиты информации. Применение теории игр к задачам обеспечения информационной безопасности открывает новые горизонты в плане повышения эффективности систем защиты, однако требует глубокого осмысления и интеграции с другими подходами для достижения синергетического эффекта [16]. Эти модели, опирающиеся на строгий математический аппарат и анализ рациональности поведения участников конфликта, предоставляют ценный инструментарий для прогнозирования действий потенциальных противников и разработки соответствующих контрмер, ориентированных на нейтрализацию угроз.

Кроме того, теоретико-игровые модели, учитывающие ограниченность ресурсов, выделяемых на обеспечение информационной безопасности, позволяют оптимизировать их распределение, максимизируя эффективность защитных мер при заданных бюджетных ограничениях, что имеет критическое значение ввиду значительных затрат, неизбежно связанных с реализацией комплексной стратегии защиты информации. Тем не менее, следует осознавать, что, несмотря на свою значимость, теоретико-игровые модели не являются универсальным решением и должны органично инте-

грироваться с другими инструментами и подходами, охватывающими как техническую составляющую, так и организационные меры, непрерывное обучение персонала, всеобъемлющий мониторинг и постоянную эволюцию процессов обеспечения безопасности, создавая целостную и адаптивную систему защиты информации, способную противостоять постоянно меняющимся угрозам в современной динамичной среде.

ЛИТЕРАТУРА

1. Аносов Р.С., Аносов С.С., Шахалов И.Ю. Формализованная риск-ориентированная модель системы информационных технологий // Вопросы кибербезопасности. 2020. №5 (39). С. 69–76.
2. Арьков П.А. Комплекс моделей для поиска оптимального проекта системы защиты информации // Известия ЮФУ. Технические науки. 2008. №8. С. 30–36.
3. Басалова Г.В. Применение методов теории игр в системах обнаружения вторжений // Известия ТулГУ. Технические науки. 2017. №10. С. 207–216.
4. Басалова Г.В., Сычугов А.А. Применение методов теории игр для оптимизации выбора средств защиты информации // Известия ТулГУ. Технические науки. 2016. №11-1. С. 122–129.
5. Белый А.Ф. Компьютерные игры для выбора методов и средств защиты информации в автоматизированных системах // Известия ЮФУ. Технические науки. 2008. №8. С. 172–176.
6. Беседина С.В., Кандудин Д.А., Муравьев В.И. Применение методов математического моделирования при обеспечении безопасности // Пожарная безопасность: проблемы и перспективы. 2019. №10. С. 37–40.
7. Быков А.Ю., Шматова Е.С. Алгоритмы распределения ресурсов для защиты информации между объектами информационной системы на основе игровой модели и принципа равной защищенности объектов // Машиностроение и компьютерные технологии. 2015. №9. С. 160–187.
8. Вахний Т.В., Гуц А.К., Бондарь С.С. Учёт вероятностей хакерских атак в игровом подходе к подбору программных средств защиты компьютерной информации // МСиМ. 2015. №3 (35). С. 91–105.
9. Вахний Т.В., Гуц А.К., Константинов В.В. Программное приложение для выбора оптимального набора средств защиты компьютерной информации на основе теории игр // Вестник ОмГУ. 2013. №4 (70). С. 201–206.
10. Вахний Т.В., Гуц А.К., Кузьмин С.Ю. Оптимальный подбор антивирусной программы и межсетевого экрана с помощью теории игр // МСиМ. 2014. №4 (32). С. 240–246.
11. Волошин И.П. Построение математической модели конфликта угроз и комплексной системы защиты информации в информационно-коммуникационных сетях // Информационная безопасность регионов. 2017. №2 (27). С. 5–8.
12. Гайнанова И.В. Применение теории игр в анализе скрытых каналов с активным противником // История и архивы. 2010. №12 (55). С. 109–116.
13. Гуц А.К., Вахний Т.В., Пахотин И.Ю. Определение оптимального набора средств защиты компьютерной системы методом Монте-Карло // МСиМ. 2018. №1 (45). С. 148–158.
14. Данеев А.В., Воробьёв А.А., Лебедев Д.М. Применение теоретико-игровых моделей для исследования качества функционирования сложных организационно-технических систем // Вестник ВИ МВД России. 2010. №4. С. 76–82.
15. Данилова О.Т., Савченко С.О., Капчук Н.В. Алгоритм построения модели нарушителя на примере системы физической защиты с применением теории игр и теории графов // ОНВ. 2017. №4 (154). С. 115–119.
16. Конюховский П., Шабалин А. Теоретико-игровые подходы в анализе стратегий защиты корпоративных информационных систем // International Journal of Open Information Technologies. 2023. №12. С. 4–15.
17. Медведев Н.В., Гришин Г.А. Оптимизация тактики защиты компьютерных сетей с использованием математического аппарата теории стратегических игр // Вестник МГТУ им. Н.Э. Баумана. Серия «Приборостроение». 2010. №4. С. 117–124.
18. Раджабова М.Т. Постановка стохастической игры защиты информации. Метод антагонистической игры двух лиц // Научные междисциплинарные исследования. 2020. №5. С. 7–11.
19. Русяев И.Л. Определение стратегии администратора по противодействию сетевым аномалиям на основе теории игр // Проблемы науки. 2017. №6 (19). С. 27–32.
20. Савченко С.О., Капчук Н.В. Алгоритм построения модели нарушителя в системе информационной безопасности с применением теории игр // ОмГТУ. 2017. №4. С. 84–89.
21. Чукляев И.И. Игровая модель обоснования применения средств комплексной защиты информационных ресурсов иерархической информационно-управляющей системы // T-Comm. 2015. №2. С. 64–68.

Журнал «Современная наука: актуальные проблемы теории и практики»