УДК

**О СВЯЗИ ПАРАДОКСОВ ТЕОРИИ ВЕРОЯТНОСТИ С ОКРУЖАЮЩЕЙ ДЕЙСТВИТЕЛЬНОСТЬЮ**

**Махонина М.А.**

**Воронежский государственный педагогический университет**

**mahoninamarina@yandex.ru**

Размышления о случайном (например, золотые правила игроков в азартные игры) были уже в древнейшие времена, но математические вычисления вероятностей и вероятностные парадоксы появляются в письменных источниках начиная лишь с XV века. Необычайным образом парадоксы могут быть связаны тем, что нас окружает, и эта взаимосвязь не всегда очевидна.

Например, парадокс азартных игр некоторым образом связан с направлениями физики XIX и XX веков. Предположим, что вместо игральной кости мы имеем дело с физическими частицами. Каждая грань кости соответствует теперь фазовой ячейке, в которой частица оказывается случайным образом и которая характеризует состояние частицы. В этом случае игра в кости эквивалентна модели Максвелла *—* Больцмана для физических частиц.

Но парадоксы теории вероятности нашли свое отражение не только в физике, но и в программировании. Так, парадокс дней рождения в общем виде применим к [хеш-функциям](https://ru.wikipedia.org/wiki/%D0%A5%D0%B5%D1%88-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D1%8F). Хеширование — преобразование [массива](https://ru.wikipedia.org/wiki/%D0%9C%D0%B0%D1%81%D1%81%D0%B8%D0%B2_(%D0%BF%D1%80%D0%BE%D0%B3%D1%80%D0%B0%D0%BC%D0%BC%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5)) входных данных произвольной длины в (выходную) [битовую](https://ru.wikipedia.org/wiki/%D0%91%D0%B8%D1%82) строку фиксированной длины, выполняемое [определённым алгоритмом](https://ru.wikipedia.org/wiki/%D0%94%D0%B5%D1%82%D0%B5%D1%80%D0%BC%D0%B8%D0%BD%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%BD%D1%8B%D0%B9_%D0%B0%D0%BB%D0%B3%D0%BE%D1%80%D0%B8%D1%82%D0%BC). Если хеш-функция генерирует *N*‑битное значение, то число случайных входных данных, для которых [хеш-коды](https://ru.wikipedia.org/wiki/%D0%A5%D0%B5%D1%88-%D0%BA%D0%BE%D0%B4) с большой вероятностью дадут [коллизию](https://ru.wikipedia.org/wiki/%D0%9A%D0%BE%D0%BB%D0%BB%D0%B8%D0%B7%D0%B8%D1%8F_%D1%85%D0%B5%D1%88-%D1%84%D1%83%D0%BD%D0%BA%D1%86%D0%B8%D0%B8) (то есть найдутся равные хеш-коды, полученные на разных входных данных), равно не 2*N*, а только около 2*N*/2. Это наблюдение используется в атаке на криптографические хеш‑функции, получившей название «[атака дней рождения](https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B0%D0%BA%D0%B0_%C2%AB%D0%B4%D0%BD%D0%B5%D0%B9_%D1%80%D0%BE%D0%B6%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F%C2%BB)».  
Существует много парадоксов и наверняка, множество их применений на практике или в других науках, однако не всегда можно легко и однозначно проследить их взаимосвязь.

**Литература**

1. Парадоксы в теории вероятностей и математической статистике / Секей Г.- М.: Мир, 1990. - 240 с.
2. Вероятность. В 2-х книгах.- 3-е изд. перераб. и доп./ Ширяев А.Н. –М.: МЦНМО, 2004. Книга 1. –520с.
3. <https://ru.wikipedia.org/wiki/Атака_>«дней\_рождения»

***Корнев Сергей Викторович***, кандидат физико-математических наук, доцент кафедры высшей математики ФГБОУ ВПО «Воронежский государственный педагогический университет», г. Воронеж.

***Махонина Марина Алексеевна***, студентка 2-го курса физико-математического факультета направления «Педагогическое образование» профилей «Математика, Информатика»