ИНФОРМАТИКА И ИНФОРМАЦИОННЫЕ ПРОЦЕССЫ / INFORMATICS AND INFORMATION PROCESSES

DOI: https://doi.org/10.60797/IRJ.2024.147.1

СОВРЕМЕННЫЕ НАПРАВЛЕНИЯ ПРИМЕНЕНИЯ КОМБИНАТОРИКИ В ОБЛАСТИ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

Научная статья

Тенячкина М.О.[1,] *, Богданова М.В.[2], Быкова К.И.[3], Сакалова К.А.[4]
[2] ORCID : 0000-0001-6769-0024;
[1, 2, 3, 4] Воронежский государственный педагогический университет, Воронеж, Российская Федерация

* Корреспондирующий автор (smol.mariya2002[at]gmail.com)

Аннотация

В современном мире все больше сфер общественной жизни подверглись процессу информатизации. Большинство областей жизни современного человека требуют использования информационных систем или использования математических методов. Комбинаторные методы издавна сопровождали жизнь человека, и на сегодняшний день активно используются в популярнейших области ИТ. Одной из наиболее распространенных является – сфера информационной безопасности. В данной статье описаны основные этапы развития комбинаторики, ее использование в различных областях жизни человека, в частности, в сфере ИТ. Представлены результаты исследования уровня информационной безопасности среди студентов, на основе которого было разработано приложение «Безопасный пароль», для возможности формирования надежных паролей студентами ВУЗа.

Ключевые слова: комбинаторика, кодирование, Python, приложение.

MODERN DIRECTIONS OF COMBINATORICS APPLICATION IN THE FIELD OF PERSONAL DATA PROTECTION

Research article

Tenyachkina M.O.[1,] *, Bogdanova M.V.[2], Bykova K.I.[3], Sakalova K.A.[4]
[2] ORCID : 0000-0001-6769-0024;
[1, 2, 3, 4] Voronezh State Pedagogical University, Voronezh, Russian Federation

* Corresponding author (smol.mariya2002[at]gmail.com)

Abstract

In the modern world, more and more spheres of social life have undergone the process of informatization. Most areas of modern human life require the use of information systems or the use of mathematical methods. Combinatorial methods have long accompanied human life, and today are actively used in the most popular areas of IT. One of the most widespread is – the sphere of information security. This article describes the main stages of development of combinatorics, its use in different areas of human life, in particular, in the IT sphere. The results of the study of information security level among students are presented, on the basis of which the application "Safe Password" was developed to enable the formation of strong passwords by university students.

Keywords: combinatorics, coding, Python, application.

Введение

Одним из крупнейших и относительно молодых разделов математики является комбинаторика. По мнению Колмогорова, «Комбинаторика – учение о числе способов, которыми можно переставить то или другое число предметов при тех или других дополнительных условиях» [2]. Комбинаторика как наука изучает дискретные объекты, множества и связи, возникающие между ними.

Изучение комбинаторики позволяет сформировать навыки решения задач, развивать логическое мышление, формировать навыки решения сложных задач.

Основные результаты

В. Я. Буняковский одним из первых определил область направления деятельности комбинаторики. По его мнению наука занимается «1) исследованием различных образов изменения порядка и мест вещей, подлежащих или не подлежащих 2 определенной зависимости, 2) разысканием законов, по которым эти изменения или перемещения могут быть измерены и вычислены, наконец, 3) приложением выводимых таким образом следствий к другим областям математики» [2]. При этом известный советский математик И.М. Гельфанд имел мнение, что комбинаторика не имеет четких границ деятельности, она охватывает всю науку, так как «все математические проблемы сводятся к комбинаторике».

Процесс рождения и становления данного раздела математики связан с именами известнейших ученых – П. Ферма, Б. Паскаля, Г.В. Лейбница, Я. Бернулли, Эйлера и др. Первоначально задачи комбинаторики касались вопросов азартных игр. Именно П. Ферма и Б. Паскаль на первых порах зарождения комбинаторики задались вопросом о решении задачи о распределении приза за победу в игре при различных условиях. Эта задача требовала посчитать количество различных комбинаций, которые бы удовлетворяли условию задачи. Именно это решение стало основой возникновения комбинаторики и теории вероятностей.

Далее крупный шаг в развитии комбинаторики делает Г.В. Лейбниц. Именно в его труде впервые был обозначен термин «комбинаторика». Лейбниц предполагал использование комбинаторики для процессов шифрования и дешифрования информации, к статистике смертности и комбинации наблюдений. «К области комбинаторики Лейбниц относил и «универсальную характеристику математику суждений, т.е. прообраз нынешней математической логики» [3]. Огромное значение в дальнейшее развитие данной области знания имел вклад Эйлера [2]. Именно его исследования стали основополагающими решений многих комбинаторных задач. «Отцом современной комбинаторики считается Пал Эрдёш» [4].

Применение комбинаторики в начале становления сводилось к использованию в процессе азартных игр. Комбинаторные способы применялись для подсчета различных комбинаций в играх в кости и карточных играх. В попытках понять, как получить ту или иную комбинацию, составлялись таблицы вариантов. На первых порах использовался лишь подсчет количества сочетаний, в последствии стала видна необходимость в учете порядка элементов в комбинации. Правила комбинаторики также использовались людьми и при игре в шахматы, которые с давних времен привлекали внимание математиков. Начало применения этого раздела математики к игре положил Эйлер в задаче о ходе коня. Главным вопросом комбинаторики было исследование конкретных позиций фигур в игре для достижения определенного результата. Подсчет возможных сочетаний, перестановок и расстановок, приводящих к победе, позволяет начинающим и опытным игрокам выработать оптимальные стратегии игры. «Как известно, основной способ поиска наилучшего хода заключается в переборе возможных ходов, рассмотрении движения по дереву последовательных позиций и оценке возникающих в результате них состояний игры» [6].

Вследствие дальнейшего развития науки с помощью комбинаторики стали решать множество практических задач, с которыми сталкивается человек в повседневной жизни. Так, хозяйки, жившие в 17 веке, столкнувшись с дефицитом тканей, были вынуждены использовать лоскутную технику шитья одежды. Для того, чтобы просчитать необходимое количество кусков ткани и составить оптимальный план их расположения хозяйкам необходимо было перебрать все возможные варианты комбинаций и выбрать наиболее подходящий. Тем самым, люди сами того не подозревая, пользовались комбинаторными правилами.

В современной жизни комбинаторные методы применяются для решения многих задач различных областей деятельности. С помощью комбинаторики в области педагогической деятельности составляются школьные расписания. При составлении необходимо учитывать не только количество дисциплин, проводимых в день, но и сочетаемость дисциплин друг с другом. Все это сводится к расчетам сочетаний с повторениями.

В медицине комбинаторика применяется при генетических исследованиях. Структура ДНК и РНК, позволяет комбинировать генные клетки и создавать элементы антител, которые возможно использовать в лекарствах. Высокие технологии позволяют использовать комбинаторику для расшифровки генетического кода, выявляя предрасположенность людей к заболеваниям различного характера возникновения.

С возникновением потребности в защите информации появилась необходимость использования комбинаторики и в области криптографии. Обеспечить надежность шифрования информации возможно лишь используя перестановки и замены букв, что опирается на комбинаторные принципы.

На сегодняшний день, вопрос безопасности и защиты информации стоит наиболее остро, так как вся наша жизнь сосредоточена вокруг социальных сетей, электронной почты, использования информации сети Интернет и различных приложений. «По данным компании ProtocomDevelopment Systems и Positive Technology, примерно: 35,4% пользователей вынуждены помнить от одного до пяти паролей; 38,1% пользователей вынуждены помнить от шести до десяти паролей; 25% пользователей постоянно забывает свои логины и пароли» [1]. Большинство посещаемых страниц сети сегодня требует создания личного аккаунта для пользования различными возможностями. Вопрос сохранения безопасности при пользовании различного рода платформами сводится к обеспечению качественной защиты паролем. Опираясь на то, что технологии вскрытия паролей ежедневно улучшаются, сохранение персональных данных требует серьезного отношения к формирования надежных логина и пароля. Ввиду того, что чаще всего взлом производится путем перебора всех возможных вариантов сочетаний, перестановок и размещений используемых символов возможно отследить возникающую у взломщиков тенденцию к вскрытию пароля. Первыми вскрываются, как правило, пароли, имеющие внутри полные слова, последовательность цифр определенного шага, не содержит в себе имя пользователя.

«В качестве кода в зависимости от рода программы могут выступать всевозможные цифры, слова или комбинации слов, поведение или действие, и так далее» [6]. В книге М. Беннета «Идеальные пароли: выбор, защита, аутентификация», автор приводит результаты статистического исследования. «Наиболее часто употребляемыми паролями являются password1, compaq, 7777777, 12345, 123456 и др.» [9]. Согласно проведенному исследованию, было выявлено, что более 75% паролей не представляют особой сложности для взлома, поскольку в них используется символы с одной раскладки. Одним из самых популярных вариантов пароля является «123456», а также различные комбинации цифр от 1 до 9.

«Несмотря на то, что некоторые ресурсы при регистрации принудительно заставляют придумать сложный пароль (требуя определенную длину пароля, наличие цифр и букв, а также специальных символов), пользователи зачастую просто стараются выполнить эти требования, не задумываясь о надежности такого пароля» [8].

«При построении шифров существенно, чтобы поиск генерировал каждый объект с линейной емкостной и временной сложностью, что, в частности, справедливо для генерации всех слов в фиксированном алфавите, а также для генерации всех элементов симметрической группы» [7]. Исходя из приведенных выше данных, комбинаторика позволяет сгенерировать надежные шифры, которые возможно использовать инструментально в качестве паролей и логинов, которые обеспечат достойный уровень безопасности для пребывающих в сети Интернет.

Так как одной из наиболее подверженных к атакам хакеров категорий являются студенты, внутри ВГПУ было проведено исследование уровня соблюдения правил информационной безопасности в сети «Интернет». Целью

данного исследования являлось исследования уровня информационной безопасности среди студентов, определение уровня осведомленности об основных принципах защиты персональных данных, выявление степени подверженности данной возрастной группы атакам хакеров. Задачами исследования стало:

– изучение соблюдения правил информационной безопасности студентами.

– определение уровня знаний студентов о методах предотвращения атак на персональные данные.

– идентификация основных проблемы и слабые места в информационной безопасности студентов.

– разработка рекомендаций по повышению осведомленности и уровня защиты персональных данных студентов.

-выявление основных принципов применения комбинаторики при составлении паролей

Исследование было осуществлено с применением комплексного, количественного подходов. Основными методами стали тестирование и анкетирование студентов 1-5 курсов физико-математического факультета. Тестирование было осуществлено по тесту «Кибербезопасность». Анкетирование включало вопросы о защищенности паролей. Проведение тестирования и анкетирования позволило получить количественные данные о знаниях и практике студентов в области безопасности и создания паролей. В результате проведенного исследования было выявлено, что 70% студентов имеют достаточный уровень грамотности в области информационной безопасности. Для выявления уровня осведомленности студентов в разрезе возраста и по мере их продвижения в учебном процессе был произведен сравнительный анализ результатов. По результатам анализа ответов студентов 1 курса и выпускников, выяснилось, что среди студентов 1-2 курсов уровень осведомленности о киберпреступлениях гораздо ниже, чем у выпускников, были выявлены некоторые «пробелы», особенно в отношении более сложных аспектов информационной безопасности, таких как защита от хакерских атак или фишинговых попыток.

При этом, анкетирование показало, что 81% опрошенных студентов хотя бы раз подвергались раскрытию пароля. Анализируя ответы, большинство студентов оценивают свой пароль как надежный (92%). При этом многие отметили, что в раскрытых паролях они использовали примитивные конструкции сочетаний символов. 62% опрошенных отметили, что использовали в пароле значимое для них слово(-а), или определенный набор цифр (дата дня рождения, дня бракосочетания и т.п.). Лишь 21% студентов ответили, что используют в пароле специальные символы – «!@№%? *#^&~{\|».

Данные анкетирования показывают, что лишь 29% людей среди опрошенных студентов не подверглись успешным атакам хакеров, среди оставшихся 81% большинство людей использовали в пароле значимые для них слова/ символы, которые остаточно легко аналитическим методом выяснить через анализ страницы личности в интернете. Большинство опрошенных (79%) также не используют для шифрации спец. символы, что ведет к упрощению вскрытия парольных данных.

«В июне 2024 года «Лаборатория Касперского» проанализировала 193 млн паролей, обнаруженных в публичном доступе на даркнет-ресурсах. Результаты исследования показали, что: почти половину из них (45%, или 87 млн.) мошенники смогут подобрать менее чем за минуту; большинство проанализированных паролей могут быть легко скомпрометированы с помощью умных алгоритмов; только 23% (44 млн.) комбинаций оказались достаточно стойкими: на их взлом ушло бы больше года».

Данное исследование подтверждает результаты проведенного опроса о ненадежности большинства парольных данных. Новизна данного исследования состоит в оно выявляет противоречие между оценкой безопасности паролей студентами и реальными практиками их использования. Несмотря на то, что большинство студентов считают свои пароли надежными, практика показывает противоположное: высокий процент студентов подвергался раскрытию паролей, а многие из них используют в паролях значимые слова или цифры, которые относительно легко вскрыть аналитическими методами. Исследование подтверждает необходимость повышения уровня осведомленности студентов о кибербезопасности и практических навыков по созданию надежных паролей.

Опираясь на результаты анкетирования, можно сделать вывод, что множество студентов, зная правила составления безопасного пароля, не применяет их в реальной практике, так как сложный пароль достаточно тяжело запомнить. Большинство использует в качестве пароля данные, которые представляют личную значимость для пользователя, что предотвращает забывание пароля, так как подобная информация легко запоминаема и воспроизводима из памяти при необходимости.

Выводы исследования демонстрируют важные тенденции и проблемы в области информационной безопасности студентов. Так как выявлено недостаточное применение принципов комбинаторики при создании паролей, различия в уровнях осведомленности кибербезопасности, были разработаны следующие практические шаги по устранению данных проблем в рамках применения внутри ВУЗа:

– Разработать обучающие программы и организовать мероприятия, направленные на повышение осведомленности студентов в области информационной безопасности.

– Внедрить обучение принципам комбинаторики при создании безопасных паролей в учебные планы для студентов.

– Усилить обучение безопасности деталей информационной безопасности на начальных курсах, чтобы предотвратить «пробелы» в понимании сложных аспектов безопасности.

– Организовать семинары и тренинги по методам создания безопасных паролей.

– Исследовать и разработать инновационные методы, способствующие запоминанию сложных и безопасных паролей с учетом особенностей студенческой аудитории.

В совокупности с описанными практическими выводами, чтобы помочь предотвращению утери пароля, упростить его запоминание и при этом обеспечить его высокую степень противостояния взлому, было разработано приложение для студентов, которое генерирует надежные пароли из перечня вводимых с клавиатуры символов. Пароли,

создаваемые приложением, сохраняют ассоциативность для конкретного пользователя, при этом имеют достаточную степень надежности.

Приложение является консольным - это «программа, которая для взаимодействия с пользователем использует консоль – клавиатуру и монитор, работающий в режиме отображения символьной информации (буквы, цифры и специальные знаки)» [5]. «Python – обширный, но в то же время довольно простой в изучении и применении язык программирования общего назначения, который часто применяют для повышения производительности разработчика кода, различный приложений и программ, написанных на данном языке, и служит для того, чтобы код был читаемым, а так как язык программирования Python довольно прост и понятен большинству начинающих программистов» [5]. Возможности данного языка очень широки. Его использование возможно при написании веб-приложений, приложений консоли, создания веб-страниц и др.

Устройство приложения имеет в себе несколько разделов. Раздел «Простой пароль» позволяет формировать пароль из введенного с клавиатуры набора символов. При выводе на экран пароля, рядом с паролем располагается шкала надежности пароля.

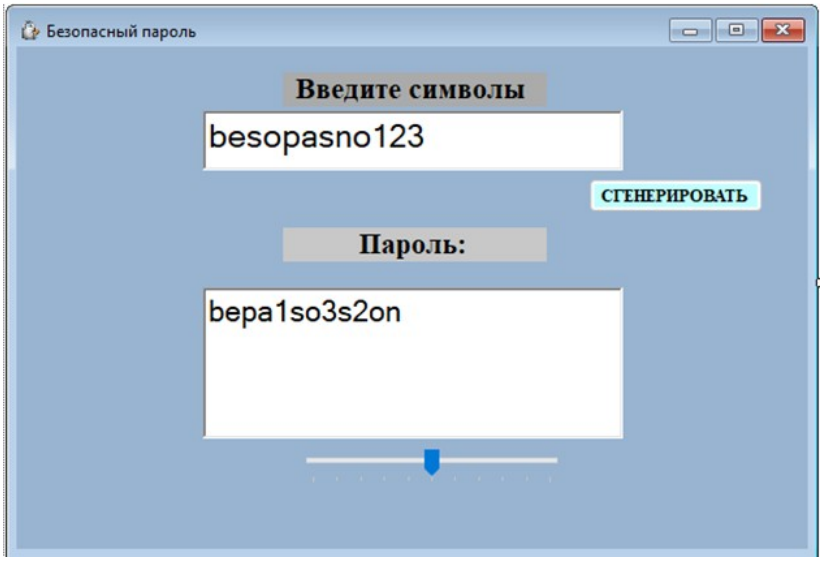

Рисунок 1 - Раздел «Простой пароль»
DOI: https://doi.org/10.60797/IRJ.2024.147.1.1

Приложение имеет в себе возможность формирования пароля из определенного набора символов, формирования пароля из нескольких строк, при этом одна из строк может быть записана в виде набора чисел. Данная возможность представлена в разделе «Сложный пароль». При данном способе формирования пароля, сначала производится формирование сочетания слов, далее к данной последовательности вместо случайно выбранных букв добавляются специальные символы, изменяется регистр некоторых букв. Еще одной возможностью приложения является оценка сформированного пароля на надежность. При этом пароль считается надежным, если не содержит данные в исходном виде, имеет изменение регистра хотя бы 2 букв, а также имеет 3 и более специальных символов.

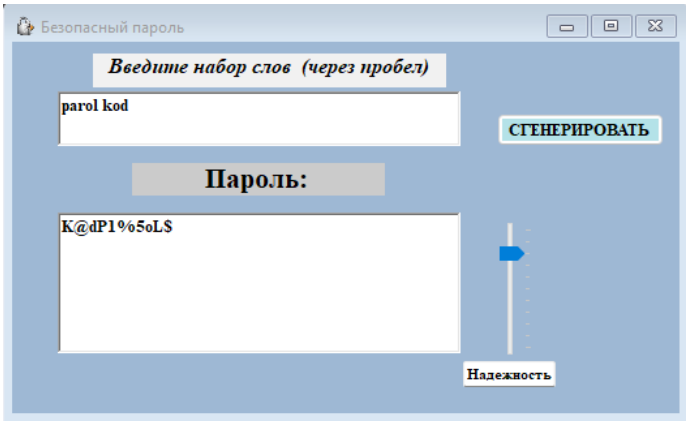

Рисунок 2 - Раздел «Сложный пароль»
DOI: https://doi.org/10.60797/IRJ.2024.147.1.2

Заключение

Подводя итог, можно сказать, что комбинаторика занимает очень важное место в современном мире. Особое значение комбинаторные методы занимают в области информационной безопасности, в частности – создании паролей, что обусловлено важностью сохранения персональных данных пользователей при широком распространении сети интернет. Опираясь на результаты исследования уровня соблюдения правил информационной безопасности в сети «Интернет», проведенного среди студентов, был выявлен недостаточный уровень защиты паролей различных сервисов. Для обеспечения безопасности, предотвращения атак хакеров, было создано приложение, базирующееся на комбинаторных правилах составления сочетаний, перемещений и размещений вводимых слов. По итогам тестирования приложения другими сервисами, создаваемые приложением пароли, действительно удовлетворяют всем критериям надежности.

Конфликт интересов

Не указан.

Рецензия

Все статьи проходят рецензирование. Но рецензент или автор статьи предпочли не публиковать рецензию к этой статье в открытом доступе. Рецензия может быть предоставлена компетентным органам по запросу.

Conflict of Interest

None declared.

Review

All articles are peer-reviewed. But the reviewer or the author of the article chose not to publish a review of this article in the public domain. The review can be provided to the competent authorities upon request.

Список литературы / References

1. Burnett M. Perfect Password: Selection, Protection, Authentication / M. Burnett // Syngress Publishing. — 2006. — № 2. — P. 178-182.
2. Веревкин А. Б. Комбинаторика. Учебное пособие / А.Б. Верёвкин. — Ульяновск, 2018. — 134 с.
3. Виленкин Н. Я. Комбинаторика / И. Я Виленкин, А. И.Виленкин, П. А Виленкин. — Москва: ФИМА, МЦНМО, 2006. — 400 с.
4. Грезина С. В. Комбинаторика и её применение / С. В. Грезина // Материалы конференции. Озёрск, 20-23 апреля 2022 г. — Озёрск: ОТИ НИЯУ МИФИ, 2022. — 92 с. — ISBN 978-5-905620-43-0
5. Ельсуков Д. А. Python – язык программирования / Д. А. Ельсуков // Экономика и социум. — 11-1(90). — 2021. — С. 982-985.
6. Как комбинаторика применяется в реальной жизни или области применения комбинаторики // Гид по играм. — URL: https://igry-gid.ru/voprosy/kak-kombinatorika-primenyaetsya-v-realnoj-zhizni-ili-oblasti-primeneniya-kombinatoriki.html (дата обращения: 27.11.2023).
7. Ковалев А. М. Модели и методы защиты информации на основе комбинаторики и хаоса / А. М. Ковалев, В. Г. Скобелев // Известия ЮФУ. Технические науки. — 2004. — №9.
8. Лим В. Б. Создание надежных паролей / В. Б. Лим // Проблемы науки. — 2021. — №3 (62).
9. Новиков В. Д. Комбинаторика для компьютерной безопасности / В. Д. Новиков, А. К. Шелехов, Е. В. Пиневич // Актуальные проблемы науки и техники. 2020: Материалы национальной научно-практической конференции, Ростов-на-Дону, 25–27 марта 2020 года / Отв. редактор Н.А. Шевченко. — Ростов-на-Дону: Донской государственный технический университет, 2020. — С. 948-950.
10. Ожигова Е. П. Об истоках символических и комбинаторных методов в конце XVIII – начале XIX в. / Е. П. Ожигова // Историкоматематические исследования. — вып. XXIV. — Москва: Наука, 1979. — С. 121-157.
11. Ускова Д. А. Применение методов комбинаторики при игре в шахматы / Д. А. Ускова // Мой первый шаг в науку: материалы II Поволжского научно-образовательного форума школьников. — Йошкар-Ола: ПГТУ, 2014. — С. 61.
12. Устюгова А. О. Решение комбинаторных задач методом перебора / А. О. Устюгова // Мой первый шаг в науку: материалы II Поволжского научно-образовательного форума школьников. — Йошкар-Ола: ПГТУ, 2014. — С. 380.

Список литературы на английском языке / References in English

1. Burnett M. Perfect Password: Selection, Protection, Authentication / M. Burnett // Syngress Publishing. — 2006. — № 2. — P. 178-182.
2. Verevkin A. B. Kombinatorika. Uchebnoe posobie [Combinatorics. Textbook] / A.B. Verevkin. — Ulyanovsk, 2018. — 134 p. [in Russian]
3. Vilenkin N. Ya. Kombinatorika [Combinatorics] / I. Ya Vilenkin, A. I.Vilenkin, P. A. Vilenkin. — Moscow: FIMA, ICNMO, 2006. — 400 p. [in Russian]
4. Grezina S. V. Kombinatorika i eyo primenenie [Combinatorics and its application] / S. V. Grezina // Materialy konferencii. Ozyorsk, 20-23 aprelya 2022 g. [Materials of the conference. Ozersk, April 20-23], 2022. — Ozersk: OTI NIYAU MEPhI, 2022. — 92 p. — ISBN 978-5-905620-43-0 [in Russian]
5. Elzhukov D. A. Python – yazyk programmirovaniya [Python is a programming language] / D. A. Zhukov // Ekonomika i socium [Economics and Society]. — 11-1(90). — 2021. — pp. 982-985. [in Russian]
6. Kak kombinatorika primenyaetsya v real'noj zhizni ili oblasti primeneniya kombinatoriki [How combinatorics takes part in real life or about the possibility of adopting combinatorics] // Gid po igram [Game Guide]. — URL: https://igry-gid.ru/voprosy/kak-kombinatorika-primenyaetsya-v-realnoj-zhizni-ili-oblasti-primeneniya-kombinatoriki.html (accessed: 27.11.2023). [in Russian]

7. Kovalev A.M. Modeli i metody zashchity informacii na osnove kombinatoriki i haosa [Models and methods of information protection based on combinatorics and chaos] // A.M. Kovalev, V. G. Skobelev // Izvestiya YUFU. Tekhnicheskie nauki [Proceedings of SFU. Technical sciences]. — 2004. — №9. [in Russian]

8. Lim V. B. Sozdanie nadezhnyh parolej [Creating strong passwords] / V. B. Lim // Problemy nauki [Problems of science]. — 2021. — №3 (62). [in Russian]

9. Novikov V. D. Kombinatorika dlya komp'yuternoj bezopasnosti [Combinatorics for computer security] / V. D. Novikov, A. K. Shelekhov, E. V. Pinevich // Aktual'nye problemy nauki i tekhniki. 2020: Materialy nacional'noj nauchno-prakticheskoj konferencii, Rostov-na-Donu, 25–27 marta 2020 goda [Actual problems of science and technology. 2020: Materials of the National Scientific and Practical Conference, Rostov-on-Don, March 25-27, 2020] / Editor N.A. Shevchenko. — Rostov-on-Don: Don State Technical University, 2020. — pp. 948-950. [in Russian]

10. Ozhigova E. P. Ob istokah simvolicheskih i kombinatornyh metodov v konce XVIII – nachale XIX v. [On the origins of symbolic and combinatorial methods at the end of the XVIII – beginning of the XIX century] / E. P. Ozhigova // Istorikomatematicheskie issledovaniya [Historicomathematical research]. — issue XXIV. — Moscow: Nauka, 1979. — pp. 121-157. [in Russian]

11. Uskova D. A. Primenenie metodov kombinatoriki pri igre v shahmaty [Application of combinatorics methods in the game of chess] / D. A. Uskova // Moj pervyj shag v nauku: materialy II Povolzhskogo nauchno-obrazovatel'nogo foruma shkol'nikov [My first step into science: materials of the II Volga Region Scientific and Educational Forum of schoolchildren]. — Yoshkar-Ola: PSTU, 2014. — p. 61. [in Russian]

12. Ustyugova A. O. Reshenie kombinatornyh zadach metodom perebora [Solving combinatorial problems by iteration method] / A. O. Ustyugova // Moj pervyj shag v nauku: materialy II Povolzhskogo nauchno-obrazovatel'nogo foruma shkol'nikov [My first step into science: materials of the II Volga Region Scientific and Educational Forum of schoolchildren]. — Yoshkar-Ola: PSTU, 2014. — p. 380. [in Russian]