инвариант данной *G*-орбиты. Предлагаемые полиномы являются своеобразными уникальными индикаторами каждой *G*-орбиты векторов-ошибок. Следовательно, полиномиальные инварианты могут служить основой обобщения ТНС, которая допускает укрупненную классификацию векторов-ошибок, то есть разбиение их на *G*-орбиты. Вычисление полиномиального инварианта очередной корректируемой ошибки позволит определить однозначно *G*-орбиту, которой принадлежит искомая ошибка. Дальнейший поиск ошибки будет проводится среди *Г*-орбит, входящих в данную *G*-орбиту. Данные обстоятельства резко сужают переборные элементы полиномиально-перестановочного алгоритма декодирования, что делает его более эффективным даже в сравнении с норменными методами.

## ОБ АЛГОРИТМЕ ПОДСЧЕТА КОЛИЧЕСТВА ОРБИТ (0,1)-МАТРИЦ

В.А. Липницкий, Н.В. Спичекова

Матрицы как двумерные массивы информации относятся к базовым объектам высшей математики. Бинарные матрицы, то есть матрицы с элементами 0 и 1, приобрели важное значение в дискретной математике, теории графов и теории групп, теории информации и помехоустойчивом кодировании, медицине и биологии. Большой вклад в исследование класса $P(n)$ квадратных (0, 1) – матриц порядка $n$, содержащих в точности $n$ единиц, внес английский математик П. Кэмерон. На исследование этого же класса матриц вышла белорусская школа помехоустойчивого кодирования [1].

Мощность класса $P(n)$ стремительно растет с ростом $n$. Например, $P(8)$ содержит 4 426 165 368 элементов. Поэтому целесообразно множес тво $P(n)$ делить на подклассы каким-то достаточно естественным образом. С середины XIX века в математике приобрела массовое применение идея разбиения множеств на орбиты – классы эквивалентности под действием на этих множествах тех или иных групп. Математические и технические приложения класса $P(n)$ показывают, что наиболее естественными преобразованиями матриц этого класса являются перестановки строк между собой или же перестановки столбцов между собой. Иными словами, наибольший интерес для пользователей представляют орбиты на множестве $P(n)$, которые образуются под действием квадрата симметрической группы. Естественным образом возникает задача о количестве таких орбит в классе $P(n)$.

Самый очевидный – переборный - способ вычисления количества орбит на множестве $P(n)$ представляет собой вычислительно сложную задачу. Поэтому применение класса $P(n)$ на практике предполагает разработку эффективных алгоритмов подсчета количества орбит этого множества. В докладе представлен реккурентный алгоритм подсчета количества орбит множества $P(n)$. Алгоритм основан на лемме Бёрнсайда [2]. Для нахождения числа матриц, инвариантных относительно действия фиксированной подстановки, используется линейная развертка бинарной матрицы. Получена оценка сложности предлагаемого алгоритма.

**Литература**

1. Цветков, В.Ю. Предсказание, распознавание и формирование образов многоракурсных изображений с подвижных объектов / В.Ю. Цветков, В.К. Конопелько, В.А. Липницкий. – Мн.: Издательский центр БГУ, 2014. – 224 с.

2. Харари, Ф. Теория графов / Ф. Харари. – М.: Мир, 1973. – 300 с.

## РАСПОЗНАВАНИЕ БИОМЕТРИЧЕСКИХ ПАРАМЕТРОВ С ПОМОЩЬЮ ЦИФРОВЫХ КАМЕР МОБИЛЬНЫХ УСТРОЙСТВ

А.М. Мажейко

Отрасль биометрического определения пользователя в информационных системах с каждым годом становится все шире и шире. Если 20 лет назад биометрические считыватели использовались исключительно в специализированных целях, то в последнее десятилетие сканеры отпечатка пальца внедряются в ноутбуки и мобильные телефоны. Однако вопрос использования еще более дешевых сканеров и методов распознавания остается открытым. Одним из самых распространенных устройств ввода на мобильных устройствах являются: микрофон и фотокамера. Исследования в Томском политехническом университете показали о

возможности эффективного распознавания ладони при анализе видеопотока камеры [1]. Это позволяет использовать цифровые камеры для получения информации о пользователе компьютера. Также в работе Бакиной И.Г. приводятся алгоритмы распознавания исключающие ошибки «склеивания пальцев» и длинных ногтей [2].

В настоящее время крупные производители компьютерной техники выпустили прототипы программного обеспечения для авторизации в системе ноутбуков. Среди них самые примечательные образцы: VeriFace от компании Lenovo, Face Recognition от Toshiba и SmartLogon от Asus. К сожалению, в алгоритмах этих программ заложены функции сравнения получаемого от камеры изображения лица с заданным образцом. Здесь высока вероятность ложного доступа в систему по представлению распечатанного изображения пользователя. Попытки устранения этой уязвимости предприняла компания NeuroTechnology в своем продукте VeriLook. Предпринятые попытки обмануть систему фотографией не увенчались успехом. Данный факт позволяет утверждать: а) технология биометрического распознавания пользователей по фото веб-камеры имеет перспективы развития; б) методика распознавания требует значительных доработок для повышения эффективности.

**Литература**

1. Нгуен Тоан Тханг. Алгоритмическое и программное обеспечение для распознавания формы руки в реальном времени с использованием SURF-дескрипторов и нейронной сети / Нгуен Тоан Тханг, В.Г. Спицын // Известия Томского политехнического университета. – 2012. – № 5 (320).

2. Бакина, И.Г. Генерация признаков для сравнения ладоней при наличии артефактов / И.Г. Бакина // Журнал «Прикладная информатика». – 2009. – № 4 (22).

## ЧИСЛЕННОЕ ОПРЕДЕЛЕНИЕ РИСКОВ БЕЗОПАСНОСТИ СВЯЗИ ИНФОКОММУНИКАЦИОННОЙ СИСТЕМЫ СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ

А.В. Макатерчик

В настоящее время значительно возрастает роль современных инфокоммуникационных систем специального назначения (ИКС СН). Развитие и совершенствование таких систем ведется в соответствии с общемировыми тенденциями. Активное внедрение новых средств связи, протоколов и инфокоммуникационных технологий привело к появлению неизученных угроз безопасности связи, возможность реализации которых злоумышленниками негативно влияет на обеспечение информационной безопасности государства и организаций различных форм собственности. Под угрозой безопасности связи понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность нанесения ущерба системе связи или ее компонентам.

Выделяют следующие виды возможных атак на ИКС СН: пассивная, активная (отказ в обслуживании, модификация потока, создание ложного потока, повторное использование). При этом реализация атаки на ИКС СН включает следующие этапы: сбор информации, выбор метода реализации и типа атаки, реализация выбранного типа атаки, завершение атаки.

На основе проведенного анализа реализации угроз информационной безопасности численное определение рисков безопасности связи для элемента ИКС СН определен способ численного определения рисков безопасности связи для элемента инфокоммуникационных систем специального назначения использованием выведенной формулы. Полученные для каждого элемента ИКС СН значения в дальнейшем используются в ходе определения численного значения рисков безопасности связи для всей ИКС СН. Предложенный подход позволяет определить численное значение рисков безопасности связи для ИКС СН с учетом как существующих, так и потенциальных уязвимостей на основе оценки мероприятий по обеспечению безопасности связи.