УДК 004.491.22

ДВУХКЛАССИФИКАЦИОННАЯ ИСКУССТВЕННАЯ ИММУННАЯ СИСТЕМА

© 2014 М.Е. Бурлаков[1]

В данной статье рассматривается практический аспект применения принципов биологической иммунной системы в решении задачи анализа и классификации электронных сообщений. В качестве анализируемых электронных сообщений брались как e-mail (электронная почта), так и сообщения из закрытых систем (электронный документооборот или систем управления бизнесом). В статье разработана двухклассификационная искусственная иммунная система с последующим сравнением эффективности ее применения с наивным байесовским классификатором. Проведена практическая реализация разработанной системы с применением в системе анализа электронных сообщений коммерческой структуры.

Ключевые слова: искусственная иммунная система, клонально-селективная теория, электронный документооборот, системы управления бизнесом, электронные сообщения, спам, классификация электронных сообщений, аффинность.

Введение

В свете развития электронно-вычислительных систем неизбежно стоит ряд задач, связанных с поиском и классификацией обрабатываемой информации. Ежедневно пользователи сталкиваются с таким понятием, как информационная перегрузка — состояние, при котором пользователь не в состоянии определить, какое сообщение для него является важным.

Системы фильтрации и поиска электронных сообщений не являются панацеей. Банальный поисковый запрос по ключевому слову, например в интернет-магазине, способен выдать информации больше, чем пользователь может обработать. Решение подобных проблем кроется в построении систем, интеллектуальных механизмов и алгоритмов, способных выдавать интересующую пользователя информацию на основе небольшого количества знаний о ней (ранее выбранный товар или сообщение, помеченное тегом ”Важно ” и т. д.). Дополнительным преимуществом подобных решений является получение информации, необходимой пользователю, но не обязательно содержащей ключевые слова, введенные ранее.

Существует множество решений, использующих те или иные алгоритмы и математические аппараты, характерные для данного типа задач. За последние десять

[1]Бурлаков Михаил Евгеньевич (knownwhat@gmail.com), кафедра безопасности информационных систем Самарского государственного университета, 443011, Российская Федерация, г. Самара, ул. Акад. Павлова, 1.

лет вышло большое количество работ, где уделяется особое внимание использованию нейронных сетей [1], генетических алгоритмов и искусственных иммунных систем (ИИС) в построении эффективных решений анализа и классификации информации [2–5]. Использование ИИС в качестве механизма классификации рассматривается в работе [6]. Однако на данный момент не разработаны эффективные механизмы классификации информации по степени важности на основе ИИС.

Цель данной работы — поиск интересующей информации на основе ожиданий и предпочтений пользователя, то есть создание системы, способной эффективно классифицировать информацию по важности с использованием ИИС, что позволит создать систему защиты от нежелательной информации.

Проблема классификации электронных сообщений

Проблема классификации электронных сообщений не имеет тривиальных решений с точки зрения применения информационных систем. Существует множество решений, каждое из которых обладает как своими плюсами, так и минусами. С одной стороны, применение байесовской логики в задаче классификации оправдано в случае достаточно большого количества сообщений, в противном случае количество ошибок первого и второго рода характеризирует систему как неэффективную. С другой стороны, применение искусственных нейронных сетей предполагает наличие базы сообщений, с помощью которой будут проводиться как обучение, так и дальнейшая тренировка применяемого алгоритма.

Совершенно новым направлением в решении данного вопроса можно выделить применение искусственных иммунных систем (ИИС) [7]. При создании соответствующих систем предъявляются определенные требования, позволяющие в конечном итоге получить систему, эффективно решающую поставленную задачу, т. е. защитить пользователя от нежелательной информации.

Требования к ИИС

Требования адаптации создаваемой системы являются критически важными и необходимым условием для ее будущей актуальности. Основные понятия и определения искусственной иммунной системы сети (ИИС) можно найти в работе Кастро [8].

Проблема классификации электронных сообщений — комплексная задача, предъявляющая ряд требований к решаемой ее системе. В случае выбора в качестве механизма решения ИИС требования к возможностям последней включают в себя:

- Хранение анализируемых объектов (электронных сообщений). Задача классификации предполагается единый формат хранения данных, на основании которого производятся как обучение ИИС, так и ее дальнейшая эксплуатация.
- Унификация данных. Существует множество видов систем обмена и передачи электронных сообщений. Для проектируемой ИИС не должно быть разницы, какой формат анализируется: будь то обычное текстовое сообщение или же мультимедийный поток данных.
- Масштабируемость обработки данных. Создаваемая система должна эквивалентно обрабатывать как небольшие объемы данных, так и их массивы. Под эквивалентностью понимается одинаковость в принципах обработки.

- Структурная масштабируемость. Наличие большого количества элементов ИИС предполагает решение задачи распараллеливания ее вычислений в рамках всей информационной системы.
- Помехоустойчивость. ИИС должна уметь качественно выделять полезные признаки из анализируемых объектов и эффективно классифицировать данные согласно поставленной задаче.
- Самоорганизация и самообучение. Момент инициализации ИИС (процесс обучения и тренировки) требует наличия стороннего учителя (пользователя). Структура ИИС должна гарантировать, что после данного процесса система подберет оптимальные для своей работы параметры, вносящие минимальные искажения в конечный результат.

Так как поставленная задача классификации формулируется путем распределения электронных сообщений на два класса: важные и неважные, предлагаемая ИИС ориентирована на работу с соответствующими двумя классами информации. Исходя из этого, рассмотрим алгоритм построения предлагаемой двухклассификационной искусственной иммунной системы.

Алгоритм двухклассификационной искусственной иммунной системы

Как упоминалось выше, задача классификации электронных сообщений заключается в перемещении последних в один из двух классов: класс важных сообщений и класс неважных сообщений. В рамках ИИС описанные классы электронных сообщений есть наборы популяций искусственных иммунных клеток. В биологическом аспекте выделяют иммуннообразующие элементы В-клетку или Т-клетку, которые обеспечивают базовую защиту организма [9]. В-клетки — функциональный тип лимфоцитов, играющих важную роль в обеспечении иммунитета. Т-клетки — клетки, обеспечивающие распознавание и уничтожение клеток, несущих чужеродные антигены.

По аналогии с биологической системой введем искусственную иммунную клетку, наследующую свойства как В-клетки, так и Т-клетки, и назовем ее β-клеткой.

Для построения ИИС для решения поставленной задачи, введем два типа β-клеток: элементарная β-клетка (далее просто β-клетка) и β-клетка с памятью (β-клетка, сохраненная в памяти ИИС из-за своей эффективности, далее β^m). Каждая β-клетка имеет свой жизненный цикл, определенный ненулевым значением возраста. Возврат β-клетки напрямую зависит от решаемой задачи. В качестве ориентира значение возраста клетки должно быть приблизительно равно мощности алфавита, для которого применяется процесс классификации, значение возраста для β^m-клетки должно быть вдвое больше значения возраста β-клетки. Возраст β-клетки в данном случае характеризуется некоторым целым ненулевым числом. Возраст β^m больше, чем возраст β-клетки, опять-таки в силу ее эффективности. В случае если возраст становится равным нулю, клетка считается умершей, и она исключается из дальнейшей работы ИИС.

Работа ИИС состоит из трех этапов: обучение (сторонний учитель), тренировка и работа. После прохождения этапа обучения каждая β-клетка будет представлять из себя пример неважного сообщения, содержащего слова из характерных полей данного электронного сообщения, которые формируют так называемый вектор сообщений (например, слова из полей "От кого", "Тема сообщения",

”Копия” и т. д.). Каждое новое сообщение, поступающее в систему, считается антигеном, и для дальнейшей классификации оно переводится в векторный формат (эквивалентный формату β-клетки) и далее подвергается процессу классификации. Если аффинность[2] между антигеном и любой β-клеткой выше некоторого порогового значения, то говорим, что β-клетка распознала антиген, и далее система маркирует сообщение его как неважное, в противном случае сообщение маркируется как важное. Следовательно, аффинность позволяет количественно оценить взаимодействие искусственных иммунных клеток.

В случае, если сообщение подтверждается позже пользователем как неважное из обработанных как важные, β-клетка трансформируется системой в β^m-клетку (при условии, что эквивалентная ей во множестве β^m-клеток не встречается), и значение ее возраста увеличивается. С целью получения новых клеток эта клетка подвергается операции клонирования и мутации. На выходе получаем конечное множество клеток, способных более эффективно распознавать новые антигены. Таким образом, постоянное создание новых β-клеток и присутствующий механизм их ликвидации (гибели) придает системе динамичность и вариативность.

Помимо этого ИИС имеет асинхронный механизм в виде анализа действий пользователя (в случае, если пользователь решит вернуть сообщения из хранилища неважных, или наоборот, переместить сообщение в важные после проведенной ранее классификации). Поскольку работа системы имеет постоянный характер, процесс самообучения и саморегуляции также не будет прерываться со временем работы. Точность анализа и принятия системой решения по входящим электронным сообщениям должна увеличиваться пропорционально количеству полученных сообщений.

Параметры двухклассификационной ИИС

Опишем ряд параметров, заложенных в двуклассификационную ИИС при проектировании:

- **Единый класс представления.** В контексте распознавания сообщений, как правило, количество важных сообщений меньше количества неважных. В данном алгоритме β-клетки представляют из себя набор неважных сообщений. Данное утверждение согласуется с биологической иммунной системой, где лимфоциты несут в себе часть антигенов.
- **Наличие генных библиотек.** Алгоритм предполагает наличие двух библиотек слов: одна содержит слова-сообщения из поля ”От кого”, другая — из поля ”Тема сообщения” и ”Копия”. В библиотеках предполагается содержание слов, которые ранее были помечены системой или пользователем как неважные. После выполнения процесса мутации слова из данных библиотек заменяются на слова из вектора признаков клетки. Отметим, что мутация в данном алгоритме предполагает замену слов на уровне самих слов, а не на уровне букв.
- **Размножение путем клонирования.** Все новые β-клетки являются клонами старых β-клеток.
- **Костимуляция.** Электронные сообщения, классифицированные как неважные, не удаляются из системы, а перемещаются в отдельную пользовательскую папку, важные сообщения доставляются пользователю в обычном порядке и алгоритм на них дальнейшего воздействия в ходе своей работы не

[2]Аффинность — мера сходства между антигеном и антителом.

оказывает. Предполагается, что система доставки сообщений оповестит двухклассификационную ИИС о новом сообщении и, таким образом, создаст первичную стимуляцию β-клеток, тогда как обратная связь от пользователя интерпретируется как сигнал костимуляции. В начальный момент работы всей системы и алгоритма, в частности, хранилище неважных сообщений может быть пусто. Действия пользователя способны вызвать ряд динамических процессов со стороны системы. Если электронное сообщение будет одобрено и перемещено двухклассификационной ИИС в неважные, а пользователю оно действительно было не интересно, то предполагается, что сигнал костимуляции уже произошел, и β-клетка увеличивает срок своей жизни на единицу. Если, с другой стороны, пользователь считает данное сообщение важным, то алгоритм выполнил неправильную классификацию, второй сигнал костимуляции не происходит, и возраст β-клетки уменьшается.

- **Две области распознавания.** За счет наличия порога аффинности вокруг каждой β-клетки существует некоторая область аффинности, в пределах которой происходит сравнение со всеми антигенами. Именно в этой области происходит стимуляция лимфоцитов β-клетки. Применение порога аффинности для повышения точности классификации недостаточно в рамках работы системы, и эмпирическим путем была установлена необходимость второй границы, называемой порогом классификации, который определяется пользователем в момент инициализации системы.
- **Процесс гибели клеток.** Для противодействия неконтролируемому росту β-клеток, вызванному процессом клонирования, и поддержанию динамического характера алгоритма в целом в алгоритме реализуется механизм гибели клеток. Так как свободные β-клетки в ходе работы алгоритма не способны доказать свою состоятельность и полезность, им дается ограниченный срок жизни, называемый возрастом. В ходе правильного определения β-клеткой характера сообщения система увеличивает ее возраст и трансформирует в β^m-клетку. β^m-клетки также могут быть уничтожены системой, однако они несут в себе полезную информацию, и, следовательно, их возраст должен быть больше β-клеток. Поэтому удаление β-клеток производится чаще, нежели β^m-клеток. Частое удаление β^m-клеток может критично сказаться на работе всего алгоритма в плане невозможности генерации на их основе новых клонов, способных хорошо распознавать антигены.

Функциональная часть двухклассификационной ИИС

Для описания функциональной части алгоритма 2КИИС определим ряд констант:

- ВК — множество свободных β-клеток. Множество ВК пусто в начале работы алгоритма.
- ВП — множество β^m-клеток. Множество ВП пусто в начале работы алгоритма.
- ТВП — количество β^m-клеток, используемых в процессе тренировки алгоритма двухклассификационной ИИС.
- УК — константа, отвечающая за уровень клонирования в ИИС алгоритме.
- УМ — константа, отвечающая за уровень мутации в ИИС алгоритме.

- ПК — пороговое значение классификации. Константа описывает значение, превышая которое сообщение считается "неважным".
- ПА — пороговое значение аффинности (превышение данного значения означает определенную неэквивалентность двух векторов, между которыми данное расстояние высчитывается).
- ВВК — начальное количество стимуляций β-клеток (возраст свободной β-клетки). Устанавливается при добавлении в систему новых β-клеток.
- ВВП — начальное количество стимуляций β^m-клеток (возраст β^m-клетки). Устанавливается при добавлении в систему новых β^m-клеток.

Представление β-клетки

Для корректной работы двухклассификационной ИИС необходимо определиться с тем, как будет представлена такая базовая величина, как β-клетка. β-клетка в данном алгоритме представлена в виде комплексного вектора. Под комплексностью вектора предполагается объединение двух или более элементарных векторов[3]:

β-клетка = <вектор1, вектор2, вектор3, ...>,
где вектор N = <слово1, слово2, слово3, ...>

Например, для электронной почты вид вектора β-клетки будет следующим:

β-клетка = <От Кого, Тема сообщения>

для системы управления предприятиям "От кого", "Тема сообщения", "Подразделение", "Копия"

β-клетка = <От Кого, Тема, Подразделение, Копия>

Содержимое каждого вектора может изменяться на протяжении всего времени работы алгоритма. Длина вектора не детерминирована, внутреннее упорядочивание слов отсутствует.

Аффинность векторов β-клеток

Под аффинностью векторов двух β-клеток будем понимать количество слов, находящихся в пересечении двух данных векторов. Данная мера используется на протяжении всей работы алгоритма. Область значений аффинного расстояния находится в промежутке [0,1]. При расчете аффинного расстояния регистр букв не учитывается, однако данная процедура чувствительна к орфографии слова.

Пусть даны две β-клетки в векторном представлении из множества ВК: ВК1 и ВК2, тогда процедура нахождения аффинного расстояния между ними рассчитывается следующим способом:

```
ПРОЦЕДУРА АффинноеРасстояние(ВК1, ВК2)
    минВектор   <- заносим вектор с равной или минимальной длиной
    максВектор  <- заносим вектор с максимальной длиной
    колво       <- количество вхождений слов минВектор в максВектор
    длина       <- длина минВектор
ВЕРНУТЬ колво/длина
```

[3]Элементарные векторы — это набор слов, взятых с того или иного характерного поля электронного сообщения ("Тема", "От кого", "Копия" и т. д.)

Практическая реализация двухклассификационной ИИС

Рассмотрим практическую реализацию алгоритмов и процедур двухклассификационной ИИС (2КИИС). Работа 2КИИС разделена на четыре этапа: инициализация, обучение, тестирование и работа. Этап работы может быть вызван в двух случаях: появление в системе новых сообщений и действие пользователя над сообщением. Общая программа 2КИИС представлена ниже:

```
ПРОГРАММА 2КИИС
    тренировкаСистемы(множество сообщений для тренировки)
    пока не пришло новое сообщение или пользователь не сделал действие
    АГ = векторСообщения    //антиген
```

```
    ЕСЛИ новое сообщение
        результат = классифицироватьСообщение(АГ)
            ЕСЛИ результат = "неважное"
                переместить сообщение в "Неважное"
        ИНАЧЕ
                показать пользователю
        ЕСЛИ действие пользователя
            обновитьПопуляцию(векторСообщения)
```

Под этапом инициализации понимается определение констант и присвоение переменных первоначальных значений. Инициализация необходима для начальной корректной работы алгоритма

Опишем процесс тренировки, классификации и обновления популяции. Задача процедуры тренировки — наполнение генной библиотеки путем использования векторов β-клеток, пригодных (отмеченных пользователем) для данного процесса (обозначим класс таких векторов слов, как ТК). Процедура подразумевает создание первоначальных β-клеток, β^m-клеток, а также применение к ним процесса клонирования и мутации.

```
ПРОЦЕДУРА тренировкаСистемы(ТК)
  ДЛЯКАЖДОГО тк из ТК
      заполняем генную библиотеку словами из вектора тк
  вырезаем произвольно ТВП из ТК и формируем из них ВП
  ДЛЯКАЖДОГО вп из ВП
      присвоить вп значение ВВП
  ДЛЯКАЖДОГО тк из ТК
      присвоить тк значение ВВК
      ДЛЯКАЖДОГО вп из ВП
          ЕСЛИ АффинноеРасстояние(вп,тк) > ПА
            МК = клонированиеМутация(вп,тк) //Мн-во клонов
            ДЛЯКАЖДОГО мк из МК
            ЕСЛИ АффинноеРасстояние(мк,вп)>=АффинноеРасстояние(вп,тк)
                  ВП = ВП U {мк}
```

Процедура тренировки описана, система готова классифицировать неизвестные входящие сообщения, а также работать с популяцией β-клеток при каком-либо

действии пользователя. Для классификации сообщения создается антиген (АГ) по тому же принципу, что и β-клетка. Далее этот антиген проходит процедуру классификации, описанную ниже:

```
ПРОЦЕДУРА классифицироватьСообщение(АГ)
        ДЛЯКАЖДОГО вк из (ВК U ВП)
                ЕСЛИ АффинноеРасстояние(АГ,вк) > ПК
                        классифицировать АГ как "неважное"
                        ВОЗВРАТ
                классифицировать АГ как "важное"
 ВОЗВРАТ
```

2КИИС использует в своей работе два сигнала. Первый сигнал появляется в том случае, если создается антиген из уже классифицированных сообщений (на которые β-клетка потратила ресурс в виде количества возбуждений или возраста), и второй сигнал приходит от пользователя в случае, если он не согласен с итогами классификации алгоритма. В ходе данного процесса остаются только те клетки, количество стимуляций которых положительно (возраст которых не равен нулю), клетки с нулевым значением удаляются из алгоритма. Антиген — сообщение, для которого уже дана реакция от пользователя.

```
ПРОЦЕДУРА обновлениеПопуляции(АГ)
        ЕСЛИ результат работы классифицироватьСообщение ИСТИНА
                ДЛЯКАЖДОГО вк из ВК
                        ЕСЛИ АффинноеРасстояние(вк,АГ) > ПА
                                Увеличить количество возбуждений вк
                максВК          <- элемент ВК аффинное расстояние которого
                                   с АГ максимально
                ВК = ВК U клониронieМутация(максВК,АГ)
                максВП          <- элемент ВП аффинное расстояние которого
                                   с АГ максимально
ЕСЛИ АффинноеРасстояние(максВК,АГ ) > АффинноеРасстояние(максВП,АГ)
        ВК = ВК \ {максВК}
        ПРИСВОИТЬ максВК значение ВВК
        ВП = ВП \ {максВП}
        ДЛЯКАЖДОГО вп из ВП
                ЕСЛИ АффинноеРасстояние(максВК, вп) > ПА
                        уменьшить кол-во возбуждений вп
        добавить слова из АГ в генную библиотеку
ИНАЧЕ
        ДЛЯКАЖДОГО вк из ВК U ВП
```

```
ЕСЛИ АффинноеРасстояние(вк, АГ) > ПА
        УДАЛИТЬ все слова вк вектора из генной библиотеки
        УДАЛИТЬ вк из системы
ДЛЯКАЖДОГО вк из ВК
        Уменьшить количество возбуждений вк вектора
ДЛЯКАЖДОГО вк из ВК U ВП
        ЕСЛИ количество возбуждений вк = 0
                удалить вк из системы
```

Опишем процедуру клонирования и мутации. Вектор ВК1 — β-клетка, которую нужно клонировать из ВК2 основываясь на их аффинном расстоянии. УК и УМ — константы, которые призваны контролировать процесс клонирования и мутации. Символ "_" в числе $\_x\_$ указывает на его нижнюю целочисленную границу (наибольшее целое число меньшее данного).

```
ПРОЦЕДУРА клонированиеМутация(ВК1,ВК2)
        афф = АффинноеРасстояние(ВК1, ВК2)
        клоны = пустое множество
        колКлонов = _афф*УК_
        колМутантов = _(1-афф)*минДлина(ВК1;ВК2)*УМ_
        ОТ 1 ДО колКлонов ДЕЛАТЬ
            квк = копия вк1
            ОТ 1 ДО колМутантов ДЕЛАТЬ
                пч = произвольное число от 1 до длина(квк)
                пс = произвольное слово из генной библиотеки
                заменяем в квк слово на пч позиции на слово пс
            ПРИСВОИТЬ количеству возбуждений константу ВВК
            клоны = клоны U {квк}
ВЕРНУТЬ клоны
```

На этом описание алгоритма 2КИИС завершено.

Эффективность 2КИИС

Для определения производительности 2КИИС алгоритма необходимо провести сравнение с другим алгоритмом, способным решать поставленную задачу по классификации электронных сообщений. Рассмотрим классический наивный байесовский классификатор (НБК). Как упоминается в работе Грехэма [10], "вероятностный подход, основанный на наивном байесовском классификаторе, остается востребованным в задаче классификации электронных сообщений". Байесовская логика была адаптирована с учетом текущей программной реализации таким же образом, как и алгоритм 2КИИС. Реализация байесовской логики основана на применении следующей формулы:

$$\nu_{\mathrm{NB}} = \arg\max_{\nu_j \in V} P(\nu_j)\Pi_i P(a_i|\nu_j), \tag{1}$$

где множество V — важные сообщения, неважные сообщения, $P(\nu_j)$ — вероятность принадлежности электронного сообщения классу V_j рассчитывается как частота вхождения класса V_j во множество тренировочных выборок. $P(a_i|\nu_j)$ — вероятность содержания слова a_i в электронном сообщении, принадлежащего классу V_j. Данная вероятность рассчитывается исходя из частоты анализируемого слова, находящегося в тренировочном массиве данных. В данном алгоритме частота слов обновляется по мере поступления информации от пользователя (аналогично тому, как это делается в алгоритме 2КИИС). Алгоритм классифицирует только те слова, которые ранее при анализе не встречались. Вероятность возникновения неизвестного слова есть ненулевая величина, равная $1/k$, где k — общее количество слов, известных системе.

Анализ эффективности 2КИИС на конкретном примере

Анализ эффективности проводился с использованием 2946 электронных сообщений, из которых 805 (27,3 %) были вручную классифицированы как неважные, оставшиеся 2141 (72,7 %) — важны. Вектор признака состоял только из слов на кириллице и/или латинице, пробелы и иные символы, отличные от указанных, исключены. Генерация псевдослучайных чисел основана на "Вихре Мерсена" и вызывается с использованием встроенной в *PHP* функции *mt_rand()*. Для работы с сообщениями использовался следующий набор параметров (табл. 1):

Таблица 1

Параметры инициализации 2КИИС алгоритма

Параметр	**Диапазон значений**	**Значение**
ТВП (начальное мн-во В-клеток в процессе тренировки 2КИИС)	>0	30
УК (уровень клонирования)	$\geqslant 1$	7,3
УМ (уровень мутации)	$\leqslant 1$	0,71
ПК (пороговое значение классификации)	[0,1]	0,25
ПА (пороговое значение аффинности)	[0,1]	0,52
ВВК (начальное количество стимуляций свободных В-клеток)	>0	130
ВВП (начальное количество стимуляций В-клеток памяти)	>0	30

Данные значения были получены в ходе проведения 200 раундов обучения и тестирования 2КИИС.

Набор параметров был получен методом экспериментального подбора и предлагает одно из наиболее оптимальных решений поставленной задачи.

Наивный байесовский классификатор обучался на первых 30 электронных сообщениях, 2КИИС — на первых 30 неважных с точки зрения пользователя сообщений. Оставшиеся сообщения использовались для тестирования.

Процесс тестирования был построен по следующей логике: после получения нового сообщения система его классифицировала и использовала полученный результат в дальнейших вычислениях. Непрерывный процесс тестирования предполагает наличие неточной оценки конечного результата. Поэтому всегда будут как минимальные, так и максимальные параметры расхождения точности. Полученное среднее значение есть среднее арифметическое всех значений. Таблица 2 показывает основные характеристики систем после прохождения этапа обучения и тестирования.

Актуальная точность показывает процент сообщений, который был классифицирован правильно как "неважные" сообщения. Из табл. 2 видно, что 2КИИС обеспечивает наиболее оптимальный баланс между процентом неважных сообщений от общего числа сообщений и актуальной точностью. Низкий процент неважных сообщений у НБК объясняется особенностью его внутренней работы: в случае если сообщение было признано неважным, характеристики данного сообщения влияют на больший объем других сообщений, нежели это есть у 2КИИС.

Таблица 2

Характеристики НБК и 2КИИС алгоритмов после этапа обучения

Алгоритм	**Общая точность классификации**	**Неинтересные сообщения от общего числа сообщений**	**Актуальная точность**
НБК	87,73 %	65,24 %	92,19 %
2КИИС	88,93 % ± 1,12 %	80,17 % ± 3,91 %	84,74 % ± 1,42 %

Рассмотрим конкретный пример, пусть слово ”акция”, встречающееся во всех электронных сообщениях, есть признак, характеризующий их как ”неважные”. Для 2КИИС данное слово будет весомым маркером, и внутри алгоритма будет создано множество как β-клеток, так и β^m-клеток, содержащих данное слово, позволяющее однозначно реагировать на новые сообщения. Для НБК рассматривается частота встречи слова ”акция”, которая может быть меньше частоты такого слова, как ”реклама”. Отсюда и более ”вялое” влияние алгоритма на подобные сообщения. Обратно, допустим, данное слово является интересным с точки зрения пользователя. 2КИИС не будет содержать никаких клеток с этим словом. НБК же будет реагировать на изменение частоты встречаемости данного слова пропорционально количеству принятых сообщений со словом ”акция”, и чем меньше сообщений, тем меньше частота и тем меньше воздействие классификатора. Только после накопления некоторого ”опыта” (например, обучение с помощью пользователя) работа НБК по классификации сообщений с данным словом будет стабильной. На рис. 1 представлено изменение точности классификации электронных сообщений с использованием алгоритмов 2КИИС и НБК. Значения для 2КИИС на рис. 1 (пунктирная кривая) есть среднее значение, полученное указанным выше способом в ходе 200 раундов обучения и тестирования, аналогичным способом получены значения с использованием НБК (сплошная кривая).

Как видно из графика, на протяжении всей работы 2КИИС демонстрирует увеличение точности классификации при падении точности у НБК, особенно при большом количестве анализируемых электронных сообщений.

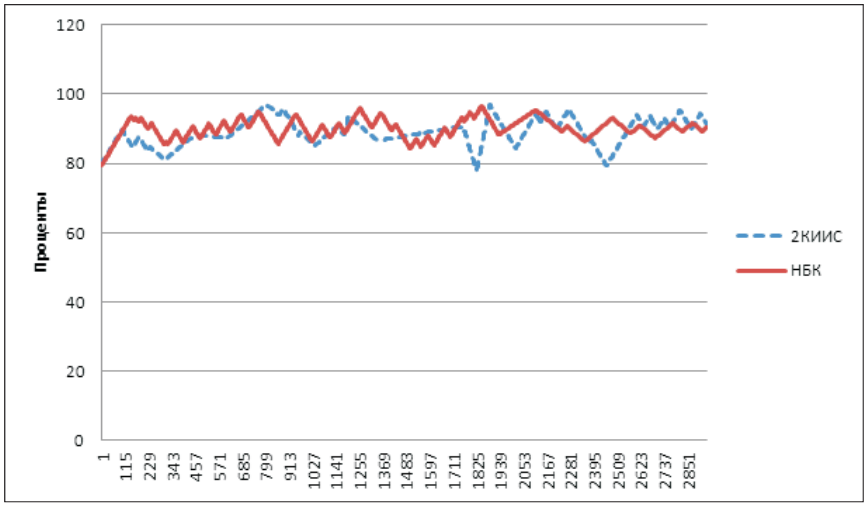

Рис. 1. Изменение точности классификации электронных сообщений

Дополнительно проводилось исследование стабильности работы алгоритмов. Суть исследования заключалась в предоставлении алгоритмам произвольных тестовых данных в процессе тестирования. Средняя точность классификации в ходе исследования у 2КИИС составила 89,1 %, НБК — 84,9 %. Однако 2КИИС показал себя более стабильным алгоритмом, т. к. в ходе тестирования значение колебания от среднего значения у НБК составило $\pm 4{,}3$ %, у 2КИИС — 1,4 %.

Исследование изменения популяции β-клеток

Дополнительно проводилось исследование изменения популяции β-клеток с целью анализа количества получаемых детектируемых элементов, необходимых для классификации электронных сообщений. На рис. 2 показано изменение общего количества β-клеток и β^m-клеток в ходе тестирования 2КИИС алгоритма в зависимости от количества принятых электронных сообщений.

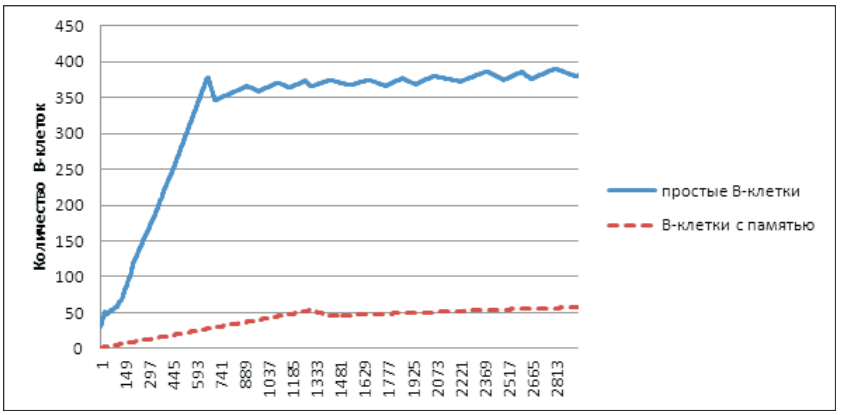

Рис. 2. Изменение популяции β-клеток в ходе классификации электронных сообщений

Как видно из рис. 2, по мере запуска процесса обучения β-клетки увеличивают свою популяцию, однако по истечении некоторого периода количество β-клеток стабилизируется. Так, после завершения активной фазы "насыщения" системы β-клетками первый максимум графика соответствует значению 378 клеток при 664 письмах, окончательное количество клеток — 381 при 2813 электронных сообщений, что соответствует несильным (не более 3 % от общего числа) колебаниям численности в ходе дальнейшей работы. Стабильность количества клеток объясняется балансировочными свойствами алгоритма (процесс гибели, коэффициенты мутации и клонирования), заложенными в предлагаемый алгоритм 2КИИС. Однако из представленных выше параметров невозможно окончательно определить среднее значение β-клеток после процесса обучения и возможные колебания их количества после "насыщения" ими системы.

Относительно β^m-клеток можно сказать, что их рост пропорционален росту количества β-клеток (рис. 2). Однако их динамика роста отличается от вышеописанной динамики и имеет более "плавный" характер роста множества β^m-клеток. Количество β-клеток многократно превышает количество β^m-клеток. В случае если бы динамика роста количества β^m-клеток соответствовала динамике роста простых β-клеток, это говорило бы о пробеле в проектировании самого алгоритма и

возможности инициации момента нестабильного роста β^m-клеток, и как следствие близкого структурного их строения между собой.

Вывод

Разработана двухклассификационная искусственная иммунная система, использующая принципы биологической иммунной системы, способная анализировать и классифицировать информацию (электронные сообщения), что позволяет защитить пользователя от несанкционированной информации.

Показана эффективность внедренной системы по сравнению с наивным байесовским классификатором (НБК), одинаково использующим принцип непрерывного обучения. Показанные результаты свидетельствуют о стабильности и эффективности системы, однако система нуждается в дальнейшей доработке и оптимизации с целью улучшения всех выходных показателей.

Литература

[1] Puniškis D., Laurutis R., Dirmeikis R. An Artificial Neural Nets for Spam e-mail Recognition, electronics and electrical engineering. Nr., 2006, Cambridge, no. 5.

[2] Burnet F.M. The Clonal Selection Theory of Acquired Immunity. Cambridge: Cambridge University Press, 1959, 312 p.

[3] Castro L., Timmis J. An Artificial Immune Network for Multimodal Function Optimization [Proceedings of IEEE Congress on Evolutionary Computation (CEC'02)], 2002, Vol. 1, pp. 699–674.

[4] Somayaji A., Hofmeyr S., Forrest S. Principles of a Computer Immune System [Proceedings of the Second New Security Paradigms Workshop], 1997, pp. 75–82.

[5] Christodorescu, Mihai, Jha, Somesh, Kruegel, Christopher. Mining specifications of malicious behavior [Proceedings of the the 6th joint meeting of the European software engineering on The foundations of software engineering], 2007, pp. 5–14.

[6] Ismaila I., Ali .S. A Spam Detection Model Based on Negative Selection Algorithm [International Journal on Data Mining and Intelligent Information Technology Applications], 2011, Vol. 2, pp. 15–17.

[7] Repository of machine learning databases. Available at: http://archive.ics.uci.edu/ml/machine-learning-databases/README (accessed: 02.05.2014).

[8] de Castro, Leandro N. Artificial Immune Systems: A New Computational Intelligence Approach. Timmis: Springer, 2004, 273 p.

[9] An artificial immune system architecture for computer security applications [IEEE Transactions on Evolutionary Computation]. Available at: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.113.9398 (accessed: 03.05.2014).

[10] A Plan for Spam. Available at: http://www.paulgraham.com/spam.html (accessed: 05.05.2014).

Поступила в редакцию 13/ *V* /2014;
в окончательном варианте — 13/ *V* /2014.

TWO-CLASSIFICATION ARTIFICIAL IMMUNE SYSTEM

© 2014 M.E. Burlakov[4]

In the article the practical aspect of application of principles of biological immune system for solving the problem of analysis and classification of email is viewed. In the capacity of analyzed emails ordinary emails (electronic mail) and mails from closed systems (electronic document flow or business management systems) were taken. In the article two-classification artificial immune system was developed with further comparison of effectiveness of their usage with naive Bayesian classification algorithm. Practical realization of the developed system with the application in the system of analysis of emails of the commercial structure is carried out.

Key words: artificial immune system, clonal selection theory, electronic document flow, business management systems, emails, spam, classification of emails, affinity.

Paper received 13/ *V* /2014.
Paper accepted 13/ *V* /2014.

[4]Burlakov Mikhail Evgenievich (knownwhat@gmail.com), the Dept. of Security of Information Systems, Samara State University, Samara, 443011, Russian Federation.