УДК 004.056

Вестник СибГАУ
2014. № 4(56). С. 41–47

# ОБНАРУЖЕНИЕ СЕТЕВЫХ ВТОРЖЕНИЙ ЭВОЛЮЦИОННЫМ ИММУННЫМ АЛГОРИТМОМ КЛОНАЛЬНОЙ СЕЛЕКЦИИ

В. Г. Жуков, Т. А. Саламатова

Сибирский государственный аэрокосмический университет имени академика М. Ф. Решетнева
Российская Федерация, 660014, г. Красноярск, просп. им. газ. «Красноярский рабочий», 31
E-mail: zhukov.sibsau@gmail.com, Shiracom@mail.ru

*Предложено применение аппарата искусственных иммунных систем в качестве эвристического метода обнаружения инцидентов информационной безопасности для алгоритмического обеспечения систем обнаружения вторжений. Из существующих вычислительных моделей искусственной иммунной системы, обладающих необходимыми особенностями для построения адаптивных систем обнаружения вторжений, выбрана теория клональной селекции. Для повышения эффективности работы (формирования высокоаффинных детекторов) предлагается модификация алгоритма клональной селекции путем применения внешней оптимизационной структуры, принцип которой основан на применении стратегии эволюционных алгоритмов. Для расчета аффинности в работе используется метрика «процент согласования». Дополнительно применяется генератор псевдослучайных чисел на основе алгоритма Блюма–Блюма–Шуба. Получены эмпирические результаты оценки эффективности эволюционного иммунного алгоритма клональной селекции при апробации на множестве тестовых данных в соответствии с методикой исследования. Проведен сравнительный анализ эффективности с аналогами разрабатываемого эволюционного иммунного алгоритма клональной селекции, построенными на других методах искусственного интеллекта. По результатам проведенных исследований сформулированы выводы об эффективности применения эволюционного иммунного алгоритма клональной селекции при решении задачи обнаружения преднамеренных изменений на множестве контролируемых данных.*

*Ключевые слова: система обнаружения вторжений, искусственные иммунные системы, алгоритм клональной селекции, эволюционная стратегия.*

Vestnik SibGAU
2014, No. 4(56), P. 41–47

# THE DETECTION OF NETWORK INTRUSION BY EVOLUTIONARY IMMUNE ALGORITHM WITH CLONAL SELECTION

V. G. Zhukov, T. A. Salamatova

Siberian State Aerospace University named after academician M. F. Reshetnev
31, Krasnoyarsky Rabochy Av., Krasnoyarsk, 660014, Russian Federation
E-mail: zhukov.sibsau@gmail.com, Shiracom@mail.ru

*In the paper the application of artificial immune systems as a heuristic detection method for algorithmic information security incidents of intrusion detection systems is proposed. A theory of clonal selection has been selected from the existing computational models of artificial immune systems with the necessary features for building adaptive intrusion detection systems. The efficiency of clonal selection algorithm is increased (forming high affinity detectors) by modification of clonal selection algorithm by applying an external structure optimization, which principle is based on the application of the evolutionary algorithm strategy. For affinity calculation in work the metrics "coordination percent" is used. Additionally, in the paper the pseudorandom numbers generator on the basis of Blum–Blum–Shub's algorithm is applied. The empirical results of the evolutionary immune clonal selection algorithm effectiveness have been received by testing on a set of test data according to the procedure of research. Comparative analysis with similar efficiency of the developed evolutionary immune clonal selection algorithm, constructed on the other methods of artificial intelligence, is performed. Conclusions on the efficiency of application of the evolutionary immune clonal selection algorithm selection at the solution of a problem of deliberate changes detection on a controlled data are formulated according to the results of the research.*

*Keywords: intrusion detection system, artificial immune systems, clonal selection algorithm, evolutionary strategy.*

**Введение.** В последние годы большое внимание уделяется вопросам защиты информации (ЗИ), накапливаемой, хранимой и обрабатываемой в информационных системах (ИС). Системы обнаружения вторжений (СОВ) являются одним из обязательных компонентов инфраструктуры безопасности ИС. Особую роль в области информационной безопасности занимают вопросы создания систем превентивной ЗИ. Благодаря свойствам и принципам работы искусственной иммунной системы (ИИС) стало возможным применение вычислительных моделей ИИС в качестве эвристического метода СОВ для обнаружения сетевых вторжений [1; 2].

Иммунная система представляет собой сложную адаптивную структуру, основная задача которой заключается в распознавании и классификации клеток (или макромолекул) организма как «своих» или «чужих». ИИС строятся по аналогии с иммунной системой живого организма с учетом различного рода допущений. Как правило, при моделировании иммунной системы используют только два центральных положениях: антиген – антитело (детектор). В настоящее время представляют интерес следующие вычислительные модели иммунных систем: алгоритмы клональной селекции и негативного отбора, иммунные сетевые алгоритмы [3].

**Алгоритм клональной селекции ИИС.** Алгоритмы клональной селекции – класс алгоритмов, использующих методы клоновой селекции и теорию приобретенного иммунитета. Клонально-селекционная теория была сформулирована в 1957 г. независимо друг от друга М. Ф. Бернетом [4] в Австралии и Д. Толмейджем [5] в США. Она объясняет, как иммунная система противостоит чужеродным макромолекулам (антигенам). Согласно теории, у каждого индивидуума система клеток, вырабатывающих антитела, еще до встречи с антигеном содержит всю информацию, необходимую для синтеза любого из самых разнообразных антител. Антиген не доставляет этим клеткам-антителам информацию, а просто отбирает те клетки, которые синтезируют соответствующие ему антитела, и побуждает их к размножению и к усиленной выработке этих антител. Клетки, синтезирующие данный вид антител, принадлежат к одному клону, слагающемуся из всех потомков одной родоначальной клетки, которая в результате случайного процесса приобрела наследственную способность реагировать на данный антиген. Пока этот антиген не появился, клон остается относительно малочисленным. Присутствие антигена стимулирует размножение клона, способного синтезировать соответствующие антитела, и чем лучше распознавание антигена, тем большее количество потомства (клонов) будет сгенерировано [6].

В процессе репродукции отдельные клетки-антитела подвергаются мутации, которая позволяет им иметь более высокое соответствие к распознаваемому антигену – *аффинность* антител. Чем выше аффинность родительской клетки, тем в меньшей степени они подвергаются мутации, и наоборот. Обучение достигается путем увеличения относительного размера популяции и аффинности тех антител, которые доказали свою ценность при распознавании представленного антигена. Каждое новое поколение содер-жит более высокое соотношение характеристик, которыми обладают лучшие члены предыдущих поколений. Схема генерации детекторов на основе алгоритма ИИС с клональной селекцией приведена на рис. 1.

По результатам проведенных исследований [7; 8] алгоритм клональной селекции ИИС позволяет обнаружить преднамеренные изменения в контролируемых данных. Основные отличия работ [7; 8] от представленных ранее – применение генератора псевдослучайных чисел на базе алгоритма Блюма–Блюма–Шуба [9] (Blum–Blum–Shub, BBS), процедуры формирования и мутации детекторов, которые в итоге позволили стабилизировать среднее количество ошибок I рода на один детектор и сделать их зависимыми от ресурсов, выделяемых алгоритму. Однако уровень ошибок I рода оставался достаточно высоким, таким образом появилась проблема формирования представительного множества высокоаффинных детекторов. В данной работе авторами предлагается повышение «качества» генерируемых детекторов за счет применения стратегии эволюционных алгоритмов.

**Модифицированный алгоритм ИИС с клональной селекцией.** Вследствие того, что ИИС относится к классу биоинспирированных алгоритмов, для формирования детекторов предлагается замещение стандартного для алгоритма клональной селекции механизма репродукции и мутации детекторов на внешнюю оптимизационную процедуру, принцип работы которой основан на применении стратегии эволюционных алгоритмов. Эволюционный алгоритм в рамках выделенного ресурса исследует пространство поиска и формирует множество высокоаффинных детекторов, итеративно улучшая их качество путем реализации принципа наследования и естественного отбора. Полученное множество детекторов ИИС используют для обнаружения антигенов. С учетом применения эволюционной стратегии модифицированный алгоритм ИИС будет иметь вид, представленный на рис. 2. Генерация детекторов производится на блок антигенов, а не на каждый отдельный антиген.

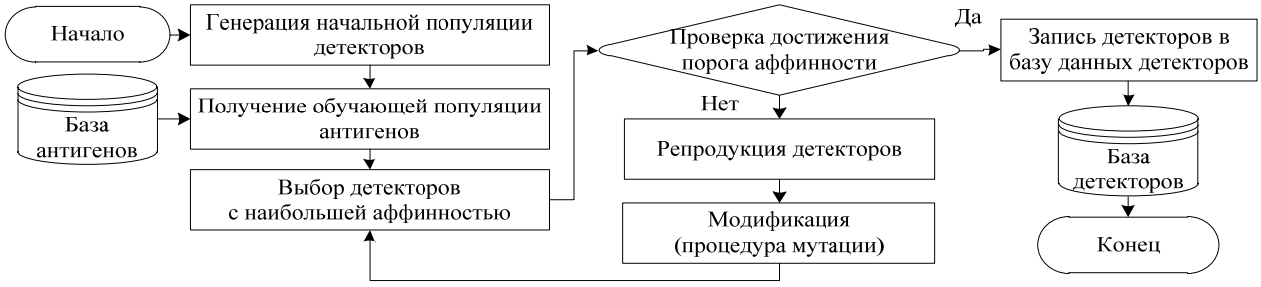


Рис. 1. Обобщенная схема генерации детекторов алгоритмом клональной селекции ИИС

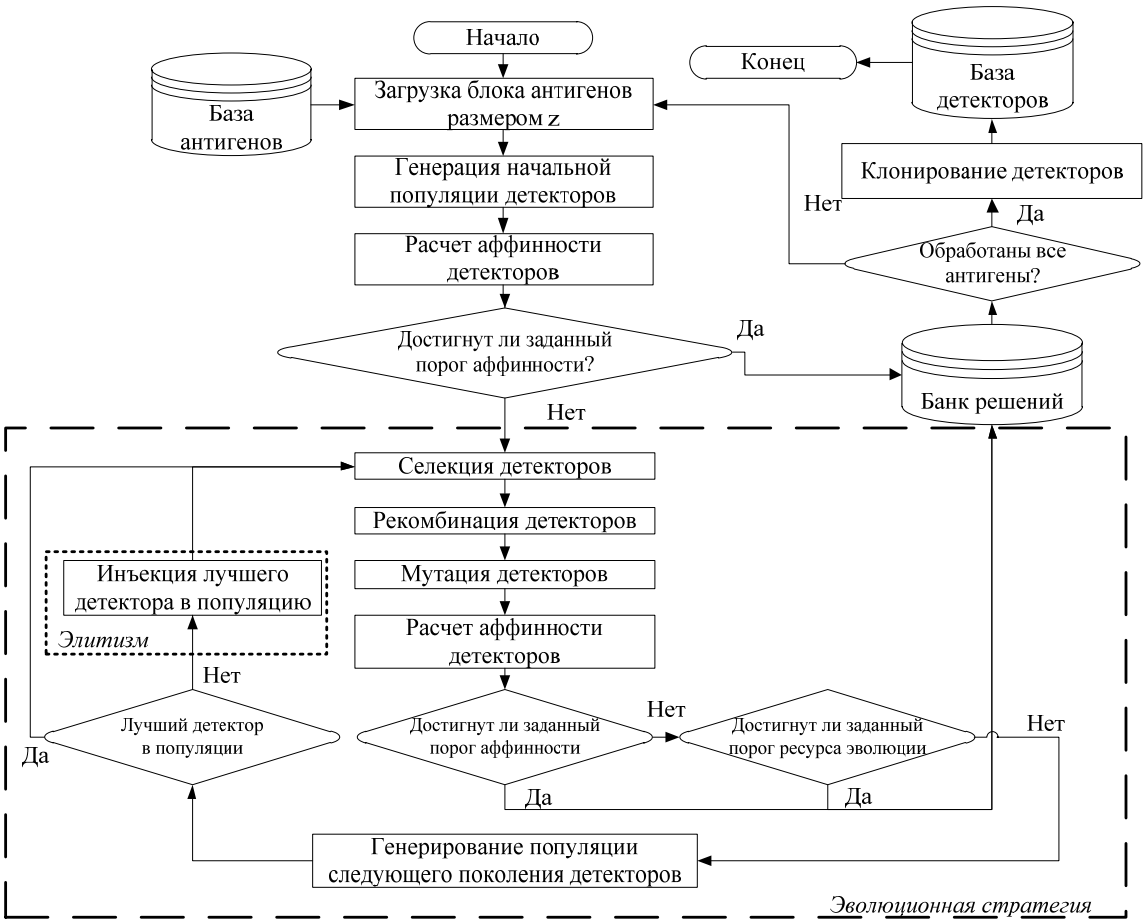


Рис. 2. Обобщенная схема генерации детекторов модифицированным алгоритмом клональной селекции ИИС

В ИИС детекторы и антигены имеют формальное представление в виде множеств элементов заданной длины над конечным алфавитом. Допустим, что мощность множеств детекторов $D$ и антигенов $A$ одинаковая и задана статично. В таком случае под аффинностью антигенов с детекторами понимается частичное или полное соответствие элемента $a_j \in A$ элементу $d_j \in D$. Аффинность растет с увеличением количества идентичных элементов и рассчитывается в данной исследовательской работе с помощью метрики «процент согласования»:

$$y = \text{count}_x\left(a[x] = d[x]\right) = \sum_{x=1}^{m} \begin{cases} 1, if\ a[x] = d[x]; \\ 0, \text{else}, \end{cases}$$

где $m=|a|=|d|$.

Функция аффинности также является функцией пригодности для эволюционного алгоритма. Генерация начальной популяции детекторов осуществляется с помощью генератора псевдослучайных чисел на основе алгоритма BBS.

На этапе селекции с помощью стратегии турнирного отбора формируется подмножество детекторов $S \subset D$, которым разрешено участвовать в формировании нового поколения детекторов.

На этапе рекомбинации с помощью генератора псевдослучайных чисел BBS выбираются два элемента из подмножества $S$, к которым применяется оператор многоточечного скрещивания по следующей схеме:

а) в диапазоне [1; $M$-1] выбираются $k$ позиций с помощью генератора псевдослучайных чисел BBS, при этом устанавливается следующее ограничение: $k \le ½ \cdot M$, где $M$ – число бит, выделенное под хранение значения детектора;

б) сгенерированные значения $k$ упорядочиваются в порядке возрастания и удаляются дублирующие значения;

в) выбранные два элемента множества $S$ обмениваются фрагментами, заключенными между соседними позициями $k$, в результате образуются детекторы-потомки.

При этом допускается, что детекторы могут представлять собой некоторую совокупность закодированных значений нескольких параметров, тогда шаги «а»–«в» оператора рекомбинации выполняются для каждого параметра отдельно. Оператор рекомбинации выполняется $|S|$ раз, в результате получаем множество детекторов-потомков мощностью, равной $|D|$.

Оператор мутации выполняется для каждого детектора-потомка с вероятностью $P_m = 1/y$, при этом используется защищенное деление.

Для формирования множества детекторов следующего поколения используется пропорциональная селекция (алгоритм «колесо рулетки»).

Следующим этапом проверяется присутствие во множестве детекторов следующего поколения лучшего детектора, обладающего самым высоким значением аффинности (принцип элитизма). В случае отсутствия такового, происходит его добавление вместо самого низкоаффинного детектора.

Процесс формирования детекторов продолжается до достижения критерия остановки работы. Критерием остановки выполнения алгоритма является достижение *p* поколений детекторов или 60%-го порога аффинности множества детекторов *D* к каждому антигену. Могут быть рассмотрены и другие значения порога аффинности, что является направлением для дальнейших исследований.

**Методика исследования эффективности модифицированного алгоритма ИИС с клональной селекцией.** Для обучения и тестирования реализованного алгоритма использовались данные, собранные Калифорнийским университетом, в общедоступной базе образцов сетевого трафика KDD Cup 1999 [10] (далее – база KDD'99). Отдельная запись KDD'99 представляется соответствием параметров состояния системы с записью о типе атаки или ее отсутствии. В единичную запись входит 41 параметр, каждый из которых характеризует состояние системы. В данной работе используется сокращенный список из 13 ключевых параметров [11]. В работе представлен фрагмент результатов исследования для данных класса Normal и данных типа Neptune класса атак DoS. Для преобразования исходных данных базы KDD'99 к унифицированному виду использовался рефлексивный двоичный код Грея [12].

Методика исследования эффективности ИИС заключается в последовательном выполнении следующих шагов:

1. Загрузка штатных событий Normal, выбранных случайно из базы KDD'99 во множество *G* с помощью генератора псевдослучайных чисел BBS мощностью *x*, где $x \in [100, 500]$ и изменяется с шагом $\tau_1 = 100$.

2. Загрузка нештатных событий (антигенов) Neptune, выбранных случайно из базы KDD'99 во множество *A* с помощью генератора псевдослучайных чисел BBS мощностью *z*, где $z \in \left[0, x/2\right]$ и изменяется с шагом $\tau_2 = 5$.

3. Формирование множества детекторов *D* мощностью 15, 20, 25 % от множества нештатных событий *A* итерационно с помощью алгоритма клональной селекции (соответственно $|D| = A \cdot 15\,\%$, $|D| = A \cdot 20\,\%$, $|D| = A \cdot 25\,\%$).

4. Формирование множества тестовых данных *E* из случайно выбранных элементов множества штатных событий *G* и нештатных событий (антигенов) *A*, так что $|E| = |G| = x$, где $x \in [100, 500]$ и изменяется с шагом $\tau_1 = 100$. Следует отметить, что для каждого значения мощности множества тестовых данных *E* количество элементов $a_j \in A$ в *E* составляет последовательно 25, 50, 75 и 100 % от *A*.

5. Множество тестовых данных *E* обрабатывается алгоритмом поиска нештатных событий с помощью элементов множества детекторов *D*.

Результатом работы алгоритма является количество обнаруженных антигенов в контролируемом множестве тестовых данных *E*, количество ошибок I рода (штатное событие детектировалось как нештатное (ложное срабатывание)) и II рода (нештатное событие детектировалось как штатное), усредненные по многократным запускам.

**Результаты экспериментальных исследований разработанного алгоритма.** На рис. 3–5 представлен сравнительный анализ результатов алгоритма клональной селекции ИИС (Алгоритм 1) с результатами работы алгоритма клональной селекции ИИС с применением эволюционной стратегии (Алгоритм 2) в зависимости от размера блока антигенов *z*.

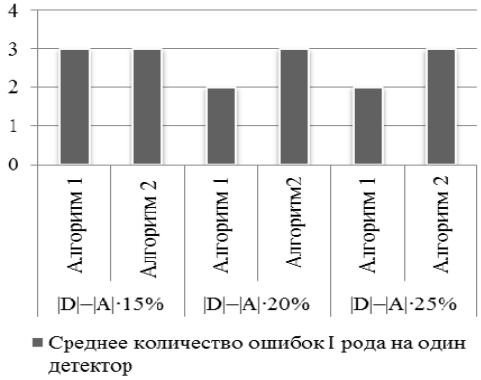


Рис. 3. Среднее количество ошибок I рода, приходящееся на один детектор при *z* = 10

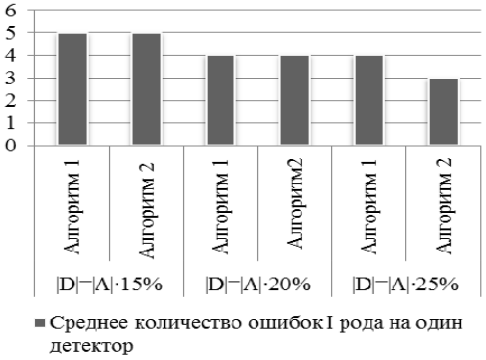


Рис. 4. Среднее количество ошибок I рода, приходящееся на один детектор при *z* = 20

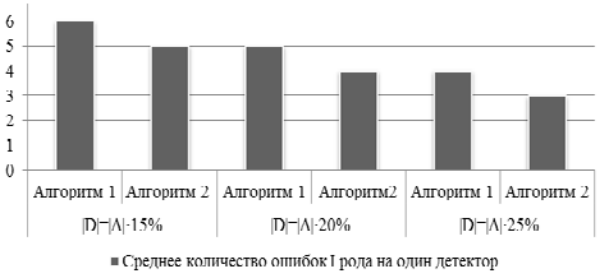


Рис. 5. Среднее количество ошибок I рода, приходящееся на один детектор при *z* = 30

Результаты экспериментов получены в процессе обнаружения антигенов в контролируемом множестве тестовых данных $E$ с помощью элементов множества детекторов $D$, в соответствии с методикой исследования эффективности, усредненных по многократным запускам. Количество запусков равно 100. Для сравнительного анализа были выбраны данные по среднему количеству ошибок I рода, приходящихся на один детектор. Ошибок II рода в процессе исследования обнаружено не было.

По результатам экспериментов (рис. 3–5) можно сделать вывод, что алгоритм клональной селекции ИИС с применением эволюционной стратегии позволяет снизить количество ошибок I рода, приходящихся на один детектор. При этом увеличение мощности множества детекторов $D$ закономерно приводит к уменьшению количества ошибок I рода независимо от размера блока антигенов $z$.

Разработанный эволюционный иммунный алгоритм клональной селекции отличается от известных тем, что для реализации стохастической процедуры поиска авторами предложено применение генератора псевдослучайных чисел на основе алгоритма Блюма–Блюма–Шуба, а для формирования высокоаффинных детекторов предлагается замещение стандартного для алгоритма клональной селекции механизма репродукции и мутации детекторов на внешнюю оптимизационную процедуру, принцип работы которой основан на применении стратегии эволюционных алгоритмов.

Предложенные модификации позволяют повысить эффективность алгоритма по критериям «Среднее количество ошибок I рода, приходящееся на один детектор» и «Среднее количество ошибок II рода, приходящееся на один детектор» по сравнению с классическим алгоритмом клональной селекции.

**Сравнение результатов тестирования модифицированного алгоритма ИИС с результатами работы алгоритмов, представленных в других работах на базе KDD'99.** Для оценки эффективности разработанного авторами алгоритма клональной селекции ИИС с применением эволюционной стратегии – эволюционного иммунного алгоритма клональной селекции – проведем сравнительный анализ результатов работы алгоритма с результатами работы различных алгоритмов на тестовом множестве KDD'99.

На рис. 6 представлены результаты сравнительного анализа с нейросетевой системой обнаружения и распознавания сетевых атак [13] (лаборатория «Искусственные нейронные сети» Брестского государственного технического университета) для моделей с различными архитектурами искусственных нейронных сетей.

На рис. 7 представлены результаты сравнительного анализа с алгоритмом на основе решающих деревьев. В основе алгоритма – модель, предложенная А. А. Брюховецким и др. (Севастопольский национальный технический университет), по обнаружению уязвимостей в критических приложениях на основе решающих деревьев [14]. В качестве критериев эффективности используются: уровень выявления атак (Detection Rate, DR), уровень пропуска атак (False Acceptence Rate, FAR), рассчитываемые по следующим формулам:

$$\mathrm{DR} = \frac{\mathrm{TP}}{\mathrm{TP}+\mathrm{FN}} \cdot 100\,\%, \quad \mathrm{FAR} = \frac{\mathrm{FP}}{\mathrm{FP}+\mathrm{TN}} \cdot 100\,\%,$$

где TP (true positive) – количество правильно определенных образцов сетевых соединений, содержащих атаку; FP (false positive) – количество образцов сетевых соединений, содержащих атаку, определенных системой как нормальные (пропуск атаки); TN (true negative) – количество правильно идентифицированных системой образцов нормальных сетевых соединений; FN (false negative) – количество нормальных образцов сетевых соединений, определенных системой как содержащие атаки.

На рис. 8 представлены результаты сравнительного анализа с результатами исследований H. M. Shirazi и другими работами [15]. H. M. Shirazi и др. предложили модель СОВ, в которой анализ собранных данных осуществляется с помощью алгоритма, построенного на основе меметического алгоритма и сетей Байеса. В качестве критерия эффективности использовался уровень выявления атак (DR).

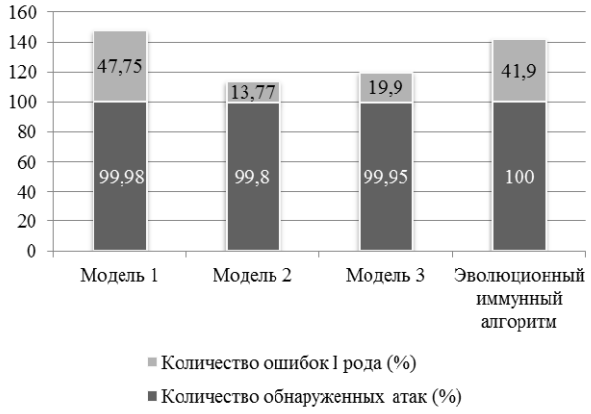


Рис. 6. Сравнительный анализ результатов работы нейросетевой системы и разработанного эволюционного иммунного алгоритма клональной селекции


Рис. 7. Сравнительный анализ результатов работы алгоритма на основе решающих деревьев и разработанного эволюционного иммунного алгоритма клональной селекции

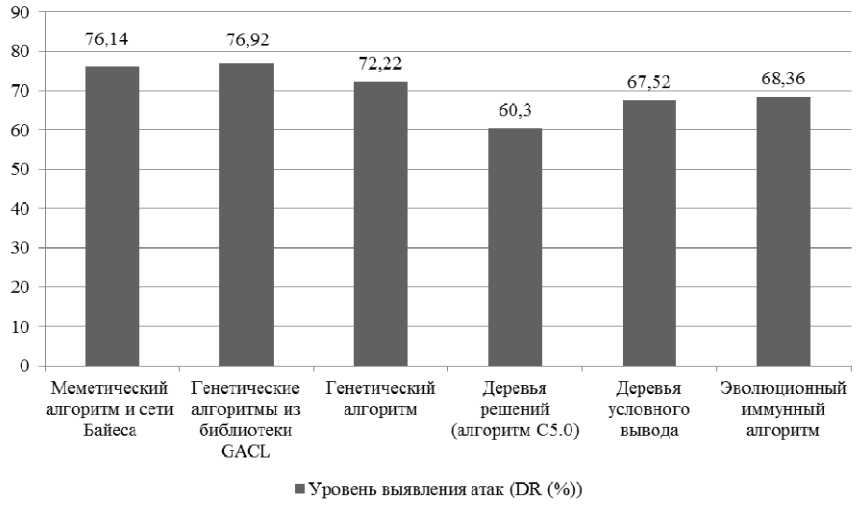


Рис. 8. Сравнительный анализ результатов исследований H. M. Shirazi
с другими работами и эволюционным иммунным алгоритмом клональной селекции

Из рис. 6–8 видно, что уровень обнаружения атак и количество ошибок I и II рода сопоставимы с аналогами, базисы которых построены на различных методах искусственного интеллекта.

**Заключение.** Замещение стандартного для алгоритма клональной селекции механизма репродукции и мутации детекторов на внешнюю оптимизационную процедуру позволило усовершенствовать процесс генерации высокоаффинных детекторов и снизить количество ошибок I рода при обнаружении вторжений.

В целом же, проанализировав полученные результаты, можно сделать вывод о том, что разработанный алгоритм позволяет обнаружить преднамеренные изменения в контролируемых данных и является перспективным базисом для разработки и совершенствования алгоритмического обеспечения эвристических методов анализа данных в задаче обнаружения сетевых вторжений в ИС, например, коллективами интеллектуальных информационных технологий или многоагентными системами, где разработанный эволюционный иммунный алгоритм клональной селекции является одним из агентов.

Построение алгоритмического обеспечения СОВ на базе эволюционного иммунного алгоритма клональной селекции позволит повысить эффективность работы СОВ в ИС с точки зрения адаптации к неизвестным угрозам ИБ.

**Благодарности.** Работа поддержана грантом Президента молодым кандидатам наук, договор № 14.124.13.473-МК от 04.02.2013 г.

**Acknowledgements.** This work was financially supported by the grant of the President of the Russian Federation for young scientists, the agreement № 14.124.13.473 – МК, d.d. 04.02.2013.

**Библиографические ссылки**

1. Dewan Md. F, Rahman M. Z., Rahman Ch. M. Mining Complex Network Data for Adaptive Intrusion Detection, Appears as a book chapter in “Data Mining/ Book 2” / Edited by Dr. Adem Karahoca. Publisher InTech, 2012.

2. A Survey of Artificial Immune System Based Intrusion Detection / H. Yang [et al.] // The Scientific World Journal. 2014.

3. Дасгупта Д. Искусственные иммунные системы и их применение : пер. с англ. М. : ФИЗМАТЛИТ, 2006. 344 с.

4. Burnet F. M. A Modification of Jerne’s Theory of Antibody Production Using the Concept of Clonal Selection // Australian Journal of Science. 1957. № 20. Pp. 67–69.

5. Talmage D. W. Allergy and Immunology // Annual Review of Medicine. 1957. № 8. Pp. 239–256.

6. De Castro L., Von Zuben F. The clonal selection algorithm with engineering applications // Proc. of GECCO’00, Workshop on Artificial Immune Systems and Their Applications. Las Vegas, 2000, P. 36–37.

7. Жуков В. Г., Саламатова Т. А. Об эффективности применения алгоритма искусственных иммунных систем с клональной селекцией в задаче автоматизированного обнаружения инцидентов информационной безопасности // Решетневские чтения : материалы XVII Междунар. науч. конф. Ч. 2 / СибГАУ. Красноярск, 2013. С. 290–292.

8. Жуков В. Г., Саламатова Т. А. Обнаружение инцидентов информационной безопасности модифицированным алгоритмом искусственной иммунной системы с клональной // В мире научных открытий : научное периодическое издание. № 6.1 (54). 2014. 497–517 с.

9. Blum L., Blum M., Shub M. A Simple Unpredictable Pseudo-Random Number Generator // SIAM Journal on Computing. 1986. Vol. 15. Pp. 364–383.

10. KDD Cup 99 Intrusion detection data set [Электронный ресурс]. URL: http://kdd.ics.uci.edu/ (дата обращения: 20.08.2014).

11. Mukkamala S., Janoski G., Sung A. Intrusion Detection: Support Vector Machines and Neural Networks [Электронный ресурс]. URL: http://www.cs.uiuc.edu/class/fa05/cs591han/papers/mukkCNN02.pdf (дата обращения: 20.08.2014).

12. Gardner M. The Binary Gray Code. Ch. 2 // Knotted Doughnuts and Other Mathematical Entertainments. New York : W. H. Freeman, 1986.

13. Технологии обнаружения сетевых атак [Электронный ресурс]. URL: http://bstu.by/~opo/ru/uni/bstu/science/ids/ (дата обращения: 20.08.2014).

14. Брюховецкий А. А., Скатков А. В., Березенко П. О. Обнаружение уязвимостей в критических приложениях на основе решающих деревьев // Современные проблемы прикладной математики, информатики, автоматизации, управления : материалы 3-го Междунар. науч.-техн. семинара. Москва : ИПИ РАН, 2013. 54–62 с.

15. Shirazi H. M., Namadchian A., Tehranikhalili A. A., Combined anomaly base intrusion detection using memetic algorithm and bayesian networks // International journal of machine learning and computing. 2012. Vol. 2, No. 5. Pp. 706–710.

**References**

1. Dewan Md. F, Rahman M. Z., Rahman Ch. M. Mining. Mining Complex Network Data for Adaptive Intrusion Detection. *Data Mining. Book 2*. August, 2012.

2. H. Yang, T. Li, X. Hu, F. Wang, Y. Zou1. A Survey of Artificial Immune System Based Intrusion Detection. *The Scientific World Journal*. 2014.

3. Dasgupta D. *Iskusstvennye immunnye sistemy i ikh primenenie* [Artificial Immune Systems and Their Applications]. Moscow, FIZMATLIT Publ., 2006, 344 p.

4. Burnet F. M. A. Modification of Jerne's Theory of Antibody Production Using the Concept of Clonal Selection. *Australian Journal of Science 20*, 1957, p. 67–69.

5. Talmage D. W. Allergy and Immunology. *Annual Review of Medicine 8*, 1957, p. 239–256.

6. De Castro L., Von Zuben F. The clonal selection algorithm with engineering applications *Proc. of GECCO'00, Workshop on Artificial Immune Systems and Their Applications*, Las Vegas, 2000, p. 36–37.

7. Zhukov V. G., Salamatova T. A. [The effective application of the artificial immune system algorithms with clonal selection in the task of information security incidents automated detection]. *Materialy XVII Mezhdunarodnoy nauchnoy konferentsii "Reshetnevskie chteniya*" [Proc. of the XVIIth *International Scientific Conference* "Reshetnev readings"], Krasnoyarsk, 2013, p. 290–292 (In Russ.).

8. Zhukov V. G., Salamatova T. A. [Detection of information security incidents modified algorithm of artificial immune system with clonal selection]. *V mire naychnikh otkritii* (*In the World of Scientific Discoveries),* Krasnoyarsk, 2014, № 6.1 (54), p. 497–517 (In Russ.).

9. Blum L., Blum M., Shub M. A Simple Unpredictable Pseudo-Random Number Generator. *SIAM Journal on Computing*, 1986, vol. 15, p. 364–383.

10. *KDD Cup 99 Intrusion detection data set.* Available at: http://kdd.ics.uci.edu/ (accessed 21 August 2014).

11. Mukkamala S., Janoski G., Intrusion Detection: Support Vector Machines and Neural Networks. *Sung A. Intrusion Detection: Support Vector Machines and Neural Networks.* Available at: http://www.cs.uiuc.edu/class/fa05/cs591han/papers/mukkCNN02.pdf (accessed 20 August 2014).

12. Gardner M. The Binary Gray Code. Ch. *2 in Knotted Doughnuts and Other Mathematical Entertainments*, New York: W. H. Freeman, 1986.

13. *Tehnologii obnaruzheniya setevih atak*. [Technology for network attacks detecting.] Available at: http://bstu.by/~opo/ru/uni/bstu/science/ids/ (accessed 10 September 2014).

14. Bryukhovetskiy A. A., Skatkov A. V., Berezenko P. O. [Detection of vulnerabilities in critical applications on the basis of decision trees. Recent developments in applied mathematics, computer science, automation]. *Materialy 3 mezhdunarodnogo nauchno-tekhnicheskogo seminara "Sovremennie problemi prikladnoi matimatiki, informatiki, avtomatizacii, upravlenia"* [Proc. of the 3rd International Scientific and Technical Workshop "Recent developments in applied mathematics, computer science, automation"], Moscow, 2013, p. 54–62 (In Russ.).

15. Shirazi H. M., Namadchian A., Tehranikhalili A. A. Combined anomaly base intrusion detection using memetic algorithm and bayesian networks. *International journal of machine learning and computing*, vol. 2, no. 5, October 2012, p. 706–710.