На правах рукописи

БУРЛАКОВ Михаил Евгеньевич

АЛГОРИТМ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ В ИНФОРМАЦИОННЫХ СЕТЯХ НА ОСНОВЕ ИСКУССТВЕННОЙ ИММУННОЙ СИСТЕМЫ

Специальность:
05.13.19 – Методы и системы защиты информации, информационная безопасность

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата технических наук

Самара – 2017

Работа выполнена на кафедре Безопасности информационных систем Федерального государственного автономного образовательного учреждения высшего образования «Самарский национальный исследовательский университет имени академика С.П. Королёва».

Научный руководитель: кандидат физико-математических наук, доцент
Осипов Михаил Николаевич

Официальные оппоненты: доктор технических наук, профессор
Сидоркина Ирина Геннадьевна
ФГБОУ ВО «Поволжский государственный технологический университет»
декан факультета информатики и ВТ

кандидат технических наук
Сенцова Алина Юрьевна
ФГБОУ ВО «Уфимский государственный авиационный технический университет»
старший преподаватель кафедры ВТ и ЗИ

Ведущая организация: ФГАОУ ВО «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики», г. Санкт-Петербург

Защита диссертации состоится 21 декабря 2017 г. в 12^{00} часов на заседании диссертационного совета Д 212.288.07 на базе ФГБОУ ВО «Уфимский государственный авиационный технический университет» по адресу: 450008, г. Уфа, ул. К. Маркса, 12.

С диссертацией можно ознакомиться в библиотеке ФГБОУ ВО «Уфимский государственный авиационный технический университет» и на сайте *www.ugatu.su*.

Автореферат разослан «___» _____ 20___ года.

Ученый секретарь
диссертационного совета,
д-р техн. наук, доцент И. Л. Виноградова

ОБЩАЯ ХАРАКТЕРИСТИКА РАБОТЫ

Актуальность темы исследования

В настоящее время, задача обеспечения информационной безопасности крайне актуальна и востребована. С каждым годом растет количество угроз, связанных с основополагающими принципами информации: доступностью, целостностью и конфиденциальностью. Постоянный прогресс в развитии антивирусов, систем обнаружения и предотвращения вторжений, межсетевых экранов, сканеров безопасности радикально не меняет общую картину в лучшую сторону.

Выделяют два сектора работы систем безопасности информации: программное обеспечение (ПО), работающее на границе «Интернет/Интранет», и ПО, работающее в локальных вычислительных сетях (ЛВС). Если для первой группы ПО существует множество рекомендаций и спецификаций, позволяющих снизить вероятность возникновения и эскалации угрозы, то для второй группы наличие высокоэффективных решений не велико.

Существует большое количество программно-аппаратных решений, позволяющих обеспечивать безопасность в ЛВС. Среди таковых решений можно выделить: комплексные системы управления безопасностью, пассивные и активные средства мониторинга доступности сетевых ресурсов, системы обнаружения и предотвращения вторжений (СОВ и СПВ). Сегодня, использование этих средств ограничено рядом факторов: сложность поддержки, высокие финансовые затраты, высокий порог вхождения специалистов, низкая эффективность перед уязвимостями «нулевого дня», высокое потребление вычислительных ресурсов и т.д.

В связи с этим, разработка более эффективных реализаций программно-аппаратных комплексов для защиты информации в ЛВС, лежащих в плоскости создания средств проактивной защиты и активного аудита, является наиболее перспективной.

Степень разработанности темы

В настоящее время в данной предметной области ведутся активные разработки как отечественных (Н.Н. Безруков, Ю.В. Бородакий, В.И. Васильев, Ю.А. Гатчин, П.Н. Девятин, В.Г. Дождиков, П.Д. Зегжда, И.В. Котенко, М.В. Кузнецов, В.Ю. Пирогов, В.А. Семеренко, Л.А. Станкевич, В.В. Сухостат, А.О. Тараканов, Л.М. Ухлинов, В.Ф. Шаньгин и др.), так и зарубежных (С. Аллексон, Д. Аллен, Д. Андерсон, Д. Деннинг, К. Лендвер, Т. Лунт, Б. Меткалф, К. Скарфоне, С. Хайкин и др.) ученых.

В то же время, выделение направления проактивной защиты позволяет решить несколько из обозначенных выше проблем путем использования технологий интеллектуального анализа данных, модульности, масштабируемости и многоагентности подхода. Поэтому выбранное для исследования направление является актуальным и представляет научный и практический интерес в области защиты информации в сетях телекоммуникаций.

Объектом исследования являются поступающие внешние запросы из Интернет пространства в локальные вычислительные системы.

Предмет исследования: искусственная иммунная система, функционирующая в качестве адаптивного компонента сетевой системы обнаружения вторжений, на примере решения задачи обнаружения аномальных запросов.

Целью диссертационной работы является повышение эффективности обнаружения угроз, представленных в виде запросов, поступающих от внешних систем в ЛВС через Интернет, на основе разработки компонента адаптивной защиты в виде искусственной иммунной системы (ИИС) для систем обнаружения вторжений.

Для достижения указанной цели в диссертации были поставлены и решены **следующие задачи**:

1. Исследование классов угроз, стадий их реализации, а также методов их обнаружения в рамках систем обнаружения вторжений, формулирование требований к адаптивным алгоритмам с целью обнаружения аномальных запросов.
2. Определение наборов данных аномальных и не аномальных запросов, исследование зависимости влияния атрибутов на общее представление запросов в наборах данных, разработка метода оптимизации атрибутного пространства у представленных экземпляров запросов.
3. Разработка метода кластеризации запросов с атрибутами, представленными в номинальных значениях с последующим выделением центров кластеров.
4. Разработка алгоритма искусственной иммунной системы для обнаружения аномальных запросов, с последующей интеграцией модели в СОВ.
5. Разработка программного комплекса системы обнаружения вторжений с внедренными адаптивными алгоритмами для детектирования аномальных запросов, анализ полученных результатов, представление рекомендаций по его практическому применению в реальных условиях эксплуатации.

Методы исследования. В работе использовались методы теории распознавания образов, теории искусственных нейронных сетей и нечеткой логики, искусственных иммунных систем, теории принятия решений и анализа соответствий, системного анализа, технологии объектно-ориентированного программирования. Для обработки результатов экспериментов использовались методы математической статистики и теории вероятностей.

Научная новизна результатов диссертации заключается в следующем:

1. Предложен метод оптимизации количества атрибутов в запросах**,** с помощью механизма анализа соответствий и вероятностных методов с получением репрезентативного набора данных для алгоритмов машинного обучения, позволяющий снизить количество анализируемых атрибутов не менее чем в 1,5 раза для эталонных наборов данных протоколов *TCP*, *HTTP/1.1* и *SMTP* и не менее чем в 2 раза для формируемых наборов данных.
2. Предложен метод кластеризации аномальных запросов с представлением атрибутов в номинальных шкалах со снижением анализируемого множества в среднем не менее чем в 2.7 раза для эталонных наборов данных протоколов *TCP*, *HTTP/1.1* и *SMTP*.

3. Предложен алгоритм ИИС по обнаружению аномальных запросов для протоколов *TCP*, *HTTP/1.1* и *SMTP* с применением механизма анализа соответствий, позволяющий повысить эффективность обнаружения угроз, по сравнению с алгоритмом логистической регрессии не менее чем на 5% и алгоритмом искусственной нейроной сети не менее чем на 4%, и уровнем ложного срабатывания не более 6%.

Теоретическая и практическая значимость результатов диссертации состоит в возможности использования разработанной системы обнаружения аномальных запросов при построении систем защиты противодействия угрозам.

Программный комплекс СОВ с интегрированной в качестве адаптивного механизма ИИС реализован для предотвращения угроз, возникающих при генерации запросов к системе через протоколы передачи информации *TCP/UDP/ICMP*, *HTTP*/1.1 и *SMTP*. Комплекс позволяет защитить пользователя в части обеспечения доступности, целостности и конфиденциальности данных, а также:

1. с высокой степенью эффективности (более 91%) обнаруживать новые, ранее неизвестные аномальные запросы по сравнению с иными применяемыми механизмами машинного обучения;

2. с высоким значением полноты и точности классификации аномальных запросов (более 96%) повысить вероятность их обнаружения.

Полученные результаты применимы как в системах обнаружения вторжений аномальных запросов, так и в системах предотвращения вторжений.

Внедрение результатов диссертационной работы.

Результаты диссертационной работы были внедрены в:

- ОАО «Оренбургнефть», г. Оренбург.
- ООО «Интеркаскад», г.Бузулук.
- ООО "Урал-Быт-Сервис", г. Бузулук.
- ООО "Ютек-НН", г. Нижний Новгород.
- АО "Институт по проектированию и исследовательским работам в нефтяной промышленности "ГИПРОВОСТОКНЕФТЬ", г. Самара.

Исследовательский прототип искусственной иммунной системы мониторинга и аудита ИС зарегистрирован в Федеральной службе по интеллектуальной собственности (№2013618955 от 09.10.2013, № 2014617066 от 10.07.2014).

Соответствие диссертации паспорту научной специальности. Содержание диссертации соответствует пункту 3 паспорта специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность» – Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса.

Достоверность результатов работы обеспечивается сравнением результатов, полученных после реализации предложенного подхода и существующих аналогов ПО, проведенным тестированием разработанного ПО в части точности вычислений и времени выполнения, корректностью математических выкладок, использованием квалифицированных экспертных оценок для проведения

вычислительных экспериментов, а также положительным эффектом от внедрения результатов работы.

Апробация работы. Основные научные и практические результаты диссертационной работы докладывались и обсуждались на международных научно-технических конференциях:

- 9-я Всероссийская школа семинар аспирантов и молодых ученых "Актуальные проблемы науки и техники", г. Уфа (2014 г.).
- XV Всероссийская научно-практическая конференция «Проблемы информационной безопасности государства, общества и личности», г. Иркутск (2014 г.).
- Международная научно-техническая конференция «Перспективные информационные технологии», г. Самара (2014 г., 2016 г. и 2017 г.).
- Конференция "Информационные технологии и нанотехнологии", г. Самара (2016 г. и 2017 г.).
- XXIV Всероссийская конференция «Структура и динамика молекулярных систем», г. Йошкар-Ола (2017 г.).

Публикации по теме диссертации. Результаты диссертационной работы отражены в 19 публикациях, в том числе 5 публикациях в рецензируемых журналах из перечня ВАК и 1 публикация в рецензируемом журнале из перечня *Scopus*. 2 свидетельства о регистрации ПО в ФИПС. Результаты по направлению диссертационной работы были представлены на Областном конкурсе «Молодой ученый года-2015» Министерства образования и науки Самарской области, где автор стал победителем.

Личный вклад автора. В диссертационной работе использованы результаты, в которых автору принадлежит определяющая роль. Часть опубликованных работ написана в соавторстве с сотрудниками научной группы. Соискатель непосредственно разработал модель искусственной иммунной системы с применением механизма анализа соответствий. Также лично автором разработаны основные методы и алгоритмы комплекса программ.

Положения, выносимые на защиту:

1. Метод оптимизации количества атрибутов запросов, основанный на применении механизма анализа соответствий и вероятностных методов с получением репрезентативного набора данных для алгоритмов машинного обучения, позволяющий снизить количество анализируемых атрибутов не менее чем в 1,5 раза для эталонных наборов данных протоколов *TCP*, *HTTP/1.1* и *SMTP* и не менее чем в 2 раза для формируемых наборов данных.

2. Метод кластеризации аномальных запросов с представлением атрибутов в номинальных шкалах позволяющий снизить размер анализируемого множества в среднем не менее чем в 2.7 раза для эталонных наборов данных протоколов *TCP*, *HTTP/1.1* и *SMTP*.

3. Алгоритм ИИС по обнаружению аномальных запросов для протоколов *TCP*, *HTTP/1.1* и *SMTP* с применением метода анализа соответствий, позволяющий повысить эффективность обнаружения угроз, по сравнению с алгоритмом

логистической регрессии не менее чем на 5% и алгоритмом искусственной нейроной сети не менее чем на 4%, и уровнем ложного срабатывания не более 6%.

4. Программный комплекс обнаружения аномальных запросов, позволяющий повысить защищенность информационной системы в части обнаружения новых угроз с использованием адаптивного механизма ИИС.

Структура и объем диссертации. Диссертация состоит из введения, четырех глав, заключения, списка литературы из 152 наименований, 5 приложений. Общий объем работы составляет 127 страниц, в том числе 13 рисунков и 37 таблиц.

ОСНОВНОЕ СОДЕРЖАНИЕ РАБОТЫ

Во введении обоснована актуальность работы; сформулированы цель и задачи исследования; приведены результаты, выносимые на защиту; отмечены их научная новизна и практическая значимость.

В главе 1 проанализированы основные аспекты, связанные с информационной безопасностью, проведено сравнение определения базового понятия угрозы безопасности информации, взятое из нескольких источников как признак наличия неоднозначности в изначальной постановке многих решаемых задач. Дополнительно рассмотрены классы угроз в рамках модели *OSI* и в части работы протоколов *TCP*, *UDP* и *ICMP* (*DoS*, *R2L*, *U2R*, *Probe*).

Описаны стадии угроз в информационных системах и сформулирована проблема обнаружения аномальных запросов системами обнаружения (СОВ, *IDS*) и предотвращения (СПВ, *IPS*) вторжений.

Выделены основные функциональные компоненты СОВ, а также рассмотрены как неадаптивные (метод графов сценариев атак, метод анализа систем состояний, экспертные системы, метод на спецификациях, сигнатурные методы), так и адаптивные методы (искусственные иммунные системы (ИИС), искусственные нейронные сети (ИНС)), применяющиеся в СОВ в качестве компонентов по обнаружению аномальных угроз и активности. Выделены основные плюсы и минусы применения ИНС и ИИС в качестве адаптивных алгоритмов в СОВ.

Определено понятие набора данных (*Datasets*), как базового критерия оценки качества работы адаптивных алгоритмов в СОВ. Приведен массив наборов данных применимых для каждого конкретного протокола, в рамках которого функционирует СОВ. Для дальнейшей работы были выбраны следующие:

- *NSL-KDD DataSet* (протоколы работы *TCP,UDP* и *ICMP*);
- *CSIC 2010* (протокол работы *HTTP/1.1*);
- *Enron Dataset* (протокол работы *SMTP*).

Определены требования к функциям адаптивных алгоритмов для обнаружения аномальных запросов (мониторинговая функция, архитектурная функция, функция хранения состояния, функция обнаружения атак, функция реагирования).

По результатам проведенных исследований были поставлены задачи по разработке адаптивных механизмов на основе ИИС в качестве компонента СОВ.

В главе 2 исследуются модели аномальных запросов и формулируется задача их обнаружения адаптивными механизмами СОВ. Для этого в качестве исследуемых наборов данных рассматриваются наборы данных из главы 1.

Определена проблема классификации запросов на два класса:

- *normal* – класс запросов, которые потенциально не опасны для конечной системы;
- *abnormal* – класс запросов, выполнение которых может привести к некорректной работе конечной системы;

с использованием двух множеств для обучения и тестирования адаптивных механизмов:

- **обучающая выборка** (*training dataset*) – на котором осуществляется подбор параметров с целью получения максимального результата в процессе формирования адаптивного алгоритма;
- **тестовая выборка** (*testing dataset*) – на котором осуществляется проверка качества обучения адаптивного алгоритма.

Подробно рассмотрен каждый набор данных с указанием соответствующих характеристик:

- ***NSL-KDD Dataset.*** Количество атрибутов – 43. Обучающая выборка: 125 973. Тестовая выборка: 22 544.
- ***CSIC 2010 HTTP***. Количество атрибутов – 18. Обучающая выборка: 119 586. Тестовая выборка: 104 001.
- ***Enron Dataset***. Количество атрибутов – 17. Обучающая выборка: 50 987. Тестовая выборка: 189 523.

Обозначена проблема оценки влияния и оптимизации количества атрибутов аномальных запросов на конечный результат тестирования адаптивных алгоритмов, ранее обученных через обучающие выборки. Для решения задачи предлагается использовать механизм множественного анализа соответствий, где аномальный *i*-ый запрос (исходный профиль объекта) *d* есть кортеж данных с представлением атрибутов в номинальных числовых величинах, который имеет следующий вид:

$$d^i = \left(d_1^i, d_2^i, \dots, d_m^i\right), \text{где } d_j^i \in 1..n_j \subset \mathbb{N}.$$

Набор кортежей представляется в виде матрицы *D*(*n, m*) размерности $n \times m$, называемой **матрицей соответствий,** где элементы d^i (аномальные запросы) ее строки, *n* – количество элементов *d* (количество аномальных запросов), *m* – количество атрибутов у элементов *d* (количество атрибутов у аномальных запросов). Под **индикаторной матрицей** *Z* понимается представление матрицы *D* в бинарном виде. Бинаризация аномальных запросов (кортежей) описывается последовательностью следующих шагов:

1. Выделяется строка-кортеж *i*-ого запроса $d^i = \left(d_1^i, d_2^i, \dots, d_m^i\right)$;

2. *j*-ая компонента кортежа $d_j^i = s$ представляется в виде последовательности бинарных значений $b_j^i = 0, \dots, 1_s, \dots, 0$ длины n_j, в котором 1 стоит на *s*-ом месте.

Таким образом, строке-кортежу d^i ставится в соответствие бинарный кортеж $z^i = \left(z_1^i, z_2^i, \dots, z_N^i\right) = \left(b_1^i, b_2^i, \dots, b_m^i\right) \in \mathbb{D}^N$, где $N = \sum_{j=1}^{m} n_j$.

Расстояние между бинарными кортежами определяется равенством (1):

$$\rho\left(z^i, z^{i'}\right)_{bin} = \sum_{j=1}^{N} \left| z_j^i - z_j^{i'} \right|. \quad (1)$$

Во множественном анализе соответствий снижение размерности пространства атрибутов производится при помощи сингулярного разложения (*singular value decomposition, SVD*) индикаторной матрицы $Z_{(n\times N)}$. Матрица $Z_{(n\times N)}$ представляется в виде:

$$Z_{(n\times N)} = U_{(n\times n)} \Lambda_{(n\times N)} V_{(N\times N)}^T,$$

где для матриц *U* и *V* выполняются условия (2) и (3):

$$U_{(n\times n)}^T U_{(n\times n)} = U_{(n\times n)} U_{(n\times n)}^T = E_{(n\times n)}, \quad (2)$$

$$V_{(N\times N)}^T V_{(N\times N)} = V_{(N\times N)} V_{(N\times N)}^T = E_{(N\times N)}, \quad (3)$$

где $E_{(n\times n)}$ – единичная матрица порядка *n*;

Λ – диагональная матрица, с элементами, удовлетворяющими условию:

$$\lambda_1 \geq \lambda_2 \geq \cdots \lambda_r > \lambda_{r+1} = \cdots = \lambda_{min(n,N)} = 0. \quad (4)$$

где $r = rank\, Z_{(n\times N)}$;

Реализация сингулярного разложения матрицы в работе опирается на следующие алгоритмы:

- алгоритм, реализованный в библиотеке *Lapack (Python)* (для квадратной невырожденной матрицы, где $rank\, Z_{(n\times N)} = min(n, N)$);
- алгоритм, реализованный в библиотеке *SVDPACK (C)* (для случая $rank\, Z_{(n\times N)} < min(n, N)$).

Дополнительно были выделены критерии анализа комбинаций атрибутов:

- Ненулевое ограничение *SVD* - ранг полученной сингулярной матрицы с учетом погрешности вычислений при реализации.
- Критерий каменистой осыпи - поиск точки, где убывание собственных значений замедляется наиболее сильно.

После применения критериев для комбинаций атрибутов и наличия метрического пространства на кортежах запросов дополнительно рассматривается процесс кластеризации. Для этого используется метод Уорда с характеристиками:

- не более 5 итераций;
- не более 5 элементов в одном кластере.

Применение множественного анализа соответствий на наборы данных дал результаты, представленные в таблицах 1, 4 и 7. В таблицах 2, 5 и 8 показаны частичные результаты значений λ_i сингулярных элементов (первые 28 из условия (4)). В таблицах 3, 6 и 9 – результаты кластеризации методом Уорда.

NSL-KDD Dataset.

Таблица 1 – Атрибуты согласно выбранным методам *NSL-KDD Dataset*

Метод	**Кол-во комбинаций атрибутов**	**% от общего числа атрибутов**	**% общего покрытия**
Ненулевое ограничение *SVD*	12 136	64%	100%
Метод каменистой осыпи	9 158	48%	97%

Таблица 2 – λ_i элементы сингулярного разложения индикаторной матрицы

114,518829	42,444582	25,260859	18,804849	15,231797	13,984953	11,2199130

10,9281900	10,0919070	9,4598370	8,7519740	8,5520310	8,2012420	8,0507690
7,8996570	7,6684320	7,3561290	6,9731140	6,7874970	6,6498500	6,5873480
6,4644990	6,3220350	6,2605470	6,2120660	6,1404730	6,1255670	6,0261060

Таблица 3 – Результирующие значения процесса кластеризации аномальных запросов методом Уорда множества *NSL-KDD Dataset*

Исходное знач. элементов	**Кол-во комбинаций атрибутов**	**Кол-во кластеров**
125 973	9 158	43 127

CSIC 2010 HTTP Dataset.

Таблица 4 – Атрибуты согласно выбранным методам

Метод	**Кол-во комбинаций атрибутов**	**% от общего числа атрибутов**	**% общего покрытия**
Ненулевое ограничение *SVD*	9758	24%	100%
Метод каменистой осыпи	6157	15%	96%

Таблица 5 – λ_i элементы сингулярного разложения индикаторной матрицы

75,083622	28,222603	7,886319	6,614172	6,587369	6,508559	6,430207
6,224692	5,759837	5,268907	4,639058	4,284249	3,956277	3,684062
3,605713	3,162278	3,093376	3,081736	2,830738	2,797854	2,786918
2,609061	2,602768	2,581218	2,54773	2,522962	2,511822	2,500624

Таблица 6 – Результирующие значения процесса кластеризации аномальных запросов методом Уорда множества *CSIC 2010 HTTP Dataset*

Исходное знач. элементов	**Кол-во комбинаций атрибутов**	**Кол-во кластеров**
119 586	6 157	33 829

Enron Dataset.

Таблица 7 – Атрибуты согласно выбранным методам

Метод	**Кол-во комбинаций атрибутов**	**% от общего числа атрибутов**	**% общего покрытия**
Ненулевое ограничение *SVD*	7681	22%	100%
Метод каменистой осыпи	5586	16%	97%

Таблица 8 – λ_i элементы сингулярного разложения индикаторной матрицы

88,8233400	33,4758790	9,1879900	7,8567410	7,7487760	7,6711420	7,5901600
7,4746840	6,6085110	5,6323800	5,3972200	4,9041610	4,7611410	4,0943760
3,9929820	3,7086630	3,5554960	3,5289380	3,3309670	3,2746950	2,9691980
2,9290360	2,8498100	2,8324360	2,7820400	2,7242360	2,7194360	2,6921450

Таблица 9 – Результирующие значения процесса кластеризации аномальных запросов методом Уорда множества *Enron Dataset*

Исходное знач. элементов	**Кол-во комбинаций атрибутов**	**Кол-во кластеров**
50 987	5 586	29 399

Анализ таблиц 1, 4 и 7 позволяет сделать вывод о том, что критерий каменистой осыпи, при значительном снижении количества комбинаций атрибутов, обеспечивает высокий процент их общего покрытия.

Метод анализа соответствий является основой процесса оптимизации атрибутного пространства на наборах данных и построения метрик для разрабатываемой ИИС.

В главе 3 разрабатываются основные элементы ИИС: формируются общие требования к ИИС (хранение анализируемых объектов, унификация данных,

масштабируемость обработки данных, структурная масштабируемость, помехоустойчивость). В качестве основных элементов ИИС задаются β-элемент и β^m-элемент – конечномерные вектора (кортежи), характеризирующие некоторые решения**.** Отличие β^m-элемента от β-элемента заключается в наличии более стабильного (оптимального) решения (под стабильным (оптимальным) решением может пониматься, например, удачная комбинация атрибутов вектора). Количество β^m-элементов по общему представлению всегда строго меньше количества β-элементов. Множество β^m-элементов называется **генной библиотекой *G.*** Множество G изначально формируется из элементов-центров кластеров после применения к ним цепочки действий «множественный анализ соответствий – сокращение атрибутов – кластеризация», рассмотренной в главе 2.

Любая ИИС W представляет собой множество β и β^m элементов, $W = B \cup B^m = (\beta_1 ... \beta_k) \cup (\beta_1^m ... \beta_s^m)$. В настоящей работе, β-элемет представляет собой пару $\beta = (c, P)$, где $c \in \mathbb{N}$ - класс элемента, $P = (p_1 ... p_n) \in \mathbb{R}^n$ – вектор в n-мерном Евклидовом пространстве.

В качестве метрики (аффинности) в ИИС выступает мера расстояния, взятая из множественного анализа соответствий. Выделяется понятие **порога аффинности (ПА)–** пороговое значение, когда β_i**-**элемент "узнает" β_j-элемент, если оба элемента относятся к одному и тому же классу и расстояние между ними не больше заданного. В качестве ПА используется соотношение (1).

Дополнительно выделяют два правила поведения ИИС W при работе с параметром порога аффинности:

- Апоптоз – если β_i-элемент "узнает" β_j-элемент, то β_j-элемент удаляется из W.
- Иммунизация – если β_i-элемент ближе к β_j-элементу, чем все остальные элементы ИИС W, то β_j-элемент добавляется к W.

А также операции:

- Мутация (*Mutating*) – процесс случайного изменения значений части атрибутов элемента. Под **коэффициентом мутации** понимается значение, указывающее количество атрибутов от общего числа, которое будет изменено. Мутация может быть выражена следующим образом:

$$Mutating(\beta = (\beta_1, \dots, \beta_n)) = (\beta_1, \dots, \beta'_{i_1}, \dots, \beta'_{i_k}, \dots, \beta_n),$$
$$k = \lfloor \varepsilon \cdot n \rfloor, \varepsilon \in [0,1],$$

где β'_i – k атрибутов вектора β – элемента, которые меняются, ε – коэффициент мутации.

- Клонирование (*Cloning*) – функция простого поэлементного "копирования" β-элемента.

Определен механизм внешнего воздействия в ИИС**,** позволяющий после стадии обучения вносить в нее новые элементы, с последующим переобучением ИИС «на лету».

Заданы этапы работы ИИС.

Этап обучения:

1. Инициализация алгоритма (задание начальных параметров и констант);

2. Формирование множества β^m-элементов через механизм анализа соответствий;

3. Увеличение их «разнообразия» через операции мутации и клонирования в ходе процесса тренировки;

4. Апоптоз и иммунизация;

5. Корректировка результатов с помощью подбора порогового значения классификации;

6. Повторение шагов 3-5 с другими значениями ПА;

7. Выбор ИИС с наиболее оптимальными результатами относительно выбранных наборов данных.

Этап классификации:

1. Отображение входного объекта с атрибутами в пространство β-элементов ИИС с нормированным бинарным представлением;

2. Определение ближайшего β^m-элемента через соотношение;

3. Назначение класса ближайшему элементу входного образа (аномальный или не аномальный запрос).

Основные моменты реализации ИИС на формальном языке программирования имеют следующий вид.

Параметры искусственной иммунной системы.

Для описания функциональной части алгоритма ИИС задается ряд констант:

- ТК – мн-во свободных β-элементов (пусто в начале работы алгоритма).
- КП – мн-во β^m-элементов (пусто в начале работы алгоритма).
- ТКП – кол-во β^m-элементов, используемых в процессе тренировки ИИС.
- УК – константа, отвечающая за уровень клонирования в ИИС.
- УМ – константа, отвечающая за уровень мутации в ИИС.
- ПА – пороговое значение аффинности.

Основная программа ИИС

```
ПРОГРАММА 2КИИС
        Инициализация() && обучениеСистемы() && тренировкаСистемы()
        Цикл "пока не пришло новое сообщение или пользователь не сделал действие"
                АГ = векторЗапроса
                ЕСЛИ новое сообщение, то результат = классифицироватьСообщение(АГ)
                        ЕСЛИ результат = False → «аномальный запрос»
                                ИНАЧЕ → Классифицировать «нормальный запрос»
                        ЕСЛИ действие обновитьПопуляцию(векторЗапроса)
```

Процедура классификации сообщения

```
ПРОЦЕДУРА классифицироватьСообщение(АГ)
        ДЛЯКАЖДОГО ск из (G' U КП)
                ЕСЛИ АффинноеРасстояние(АГ,ск) > ПА
                        классифицировать АГ как «аномальный» и ВОЗВРАТ
                классифицировать АГ как «не аномальный»
```

Процедура обновления популяции

```
ПРОЦЕДУРА обновлениеПопуляции(АГ)
        ЕСЛИ результат работы классифицироватьСообщение ИСТИНА
                макс ТК  <-  элемент ТК  расстояние которого с АГ максимально
                ТК = ТК U клониронieМутация(макс ТК,АГ)
                макс КП  <-  элемент КП  расстояние которого с АГ максимально
ЕСЛИ АффинноеРасстояние(макс ТК,АГ ) > АффинноеРасстояние(макс КП,АГ)
        ТК = ТК \ {макс ТК} и КП = КП U {макс ТК} и          добавить АГ в генную библиотеку G
ИНАЧЕ
        ДЛЯКАЖДОГО  тк из ТК U КП
                ЕСЛИ  АффинноеРасстояние(тк, АГ) > ПА →  УДАЛИТЬ тк из системы
```

Процедура клонирования и мутации

```
ПРОЦЕДУРА клонироанieМутация(ВК1,ВК2, клоны = Array())  : ВЕРНУТЬ клоны
        афф = АффинноеРасстояние(ВК1, ВК2)
        колКлонов = _афф*УК_
        колМутантов = _(1-афф)*расстояние(ВК1;ВК2)*УМ_
        ОТ 1 ДО колКлонов ДЕЛАТЬ
                        пч = произвольное число* от 1 до длина(ВК1)
                        пс = произвольное слово из генной библиотеки G
                        заменяем в кск слово на пч позиции на слово пс
                ПРИСВОИТЬ количеству возбуждений константу ВСК и клоны = клоны U {кск}
```

На основании представленного, разработана программная реализация алгоритма ИИС для последующего исследования в качестве адаптивного компонента СОВ.

В главе 4 решаются вопросы реализации методов и алгоритмов обнаружения аномальных запросов с использованием в качестве адаптивного механизма предложенного алгоритма ИИС («СОВ ИИС»). Для разработки программного комплекса «СОВ ИИС» сформирована блок-схема модулей и подсистем.

На рисунке 1 изображена архитектура функционирования подсистемы обучения и классификации аномальных запросов, реализующая в себе предложенные выше методы и алгоритмы.

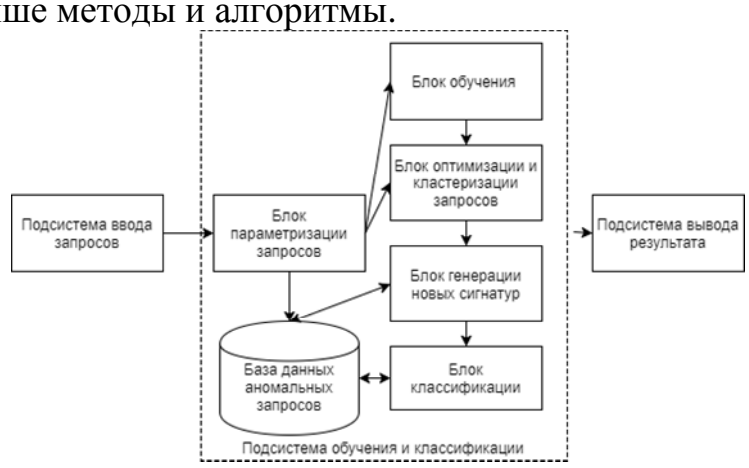

Рисунок 1 – Архитектура подсистемы обучения и идентификации аномальных запросов

Для сведения описанных выше блоков и подсистем в единый комплекс предложена схема функционирования ПО «СОВ ИИС» (рисунок 2).

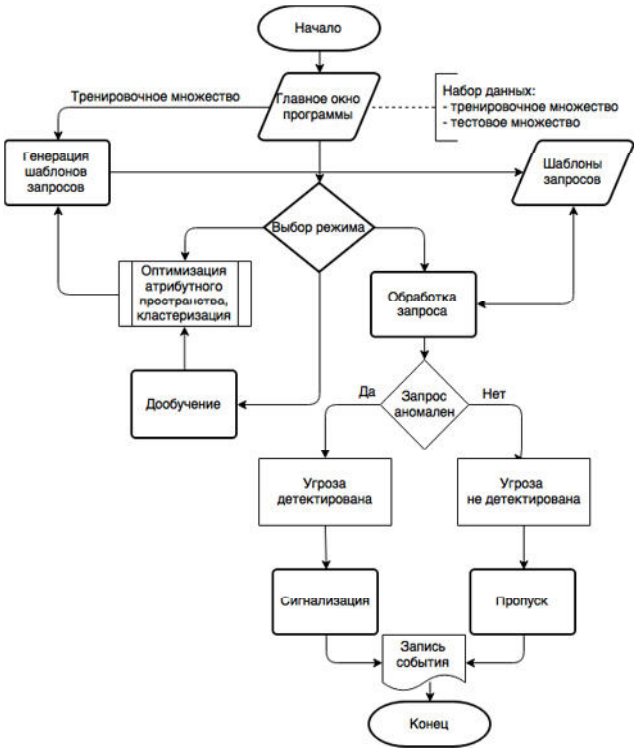

Рисунок 2 – Блок-схема функционирования комплекса «СОВ ИИС»

Помимо схемы функционирования «СОВ ИИС», задается формальный алгоритм обучения и тестирования:

Шаг 1. Берется исследуемое множество запросов с дальнейшим разбиением на два подмножества (выборки): обучающее и тестовое.

Шаг 2. Формируются кортежи запросов с атрибутным пространством признаков.

Шаг 3. Бинаризация кортежей и создание из них прямоугольной матрицы.

Шаг 4. Методом *SVD* выводится матрица Λ, состоящая из данных, полученных на **Шаге 3**, формируются наиболее значимые комбинации атрибутов.

Шаг 5. Выделяются наиболее значимые атрибуты, производится процесс кластеризации запросов с последующим выделением центров кластеров в отдельное множество (генная библиотека G).

Шаг 6. С помощью получившегося на **Шаге 5** множества запросов и ИИС генерируется новое множество аномальных запросов (множество G').

Шаг 7. С использованием обратного преобразования сингулярного разложения, а также метода округления *round*, элементы множеств G и G' преобразуются в аномальные запросы с исходными (как на *Шаге 1*) атрибутами из атрибутного пространства признаков.

Шаг 8. С использованием тестового множества аномальных запросов, проводится оценка эффективности работы алгоритма.

Критерии оценки работы СОВ лежат в плоскости минимизации с использованием ошибок первого (*false negative*, *FN*) и второго рода (*false positive, FP*). Дополнительно для оценки количества правильно классифицированных запросов используются параметры:

Уровень истинно положительных сигналов: $R_{TP} = \frac{N_{TP}}{N_{TP}+N_{FN}}$,

где N_{TP} *(true positive)* – правильно классифицированные аномальные запросы, N_{FN} *(false negative)* – ошибочно определенные аномальные сигналы.

Уровень ложно положительных сигналов: $R_{FP} = \frac{N_{FP}}{N_{FP}+N_{TN}}$,

где, N_{FP} *(false positive)* – ошибочно определенные не аномальные запросы, N_{TN} (*true negative*) – правильно классифицированные не аномальные запросы.

Точность: $P = \frac{N_{TP}}{N_{TP}+N_{FP}}$. **$F$-мера:** $F = 2\frac{P \cdot R_{TP}}{P+R_{TP}}$.

Проверка эмпирического анализа эффективности проводилась с применением техники *k*-ступенчатой кросс-валидации: каждый опыт проводился 100 раз и в качестве результата принималось среднее арифметическое.

Приведены сравнения ИИС с классификаторами на основе алгоритма логистической регрессии и на основе ИНС.В качестве показателей эффективности моделей машинного обучения используются следующие характеристики:

1. C_0 – процент корректно классифицированных не аномальных запросов;
2. C_1 – процент корректно классифицированных аномальных запросов;
3. R_{TP} – уровень истинно положительных сигналов;
4. R_{FP} – уровень ложных срабатываний;
5. P – точность системы.
6. F – F-мера, дающая общую оценку классификатора с точки зрения точности и полноты.

В [Таблица 10], представлены результаты применения алгоритмов машинного обучения для выбранных *Dataset*'ов.

Таблица 10 – Результаты работы классификаторов на основе алгоритма логистической регрессии (ЛР), ИНС и ИИС

		Оптимизация атрибутов	C_0(%)	C_1(%)	R_{TP}(%)	R_{FP}(%)	P(%)	F(%)
ЛР	*NSL-KDD DataSet*	-	86	78	86	15	88	84
		+	83	75	84	17	87	83
	CSIC 2010	-	86	92	92	14	89	91
		+	82	90	89	18	86	90
	Enron Dataset	-	85	85	90	15	87	89
		+	83	83	88	17	85	87
ИНС	*NSL-KDD DataSet*	-	87	89	87	13	88	90
		+	84	87	86	16	84	87
	CSIC 2010	-	86	96	92	14	88	91
		+	82	95	89	18	86	90
	Enron Dataset	-	85	95	90	15	88	90
		+	82	92	87	18	85	89

		Aff.	β^m/β (%)	Оптимизация атрибутов	C_0(%)	C_1(%)	R_{TP}(%)	R_{FP}(%)	P(%)	F(%)

ИИС	*NSL-KDD DataSet*	0.01	22	-	98	96	96	2	97	96
			22	+	97	94	94	3	96	94
		0.05	19	-	96	94	93	4	95	94
			18	+	94	92	91	6	93	92
		0.1	16	-	95	91	90	5	93	92
			15	+	93	90	88	7	92	91
	CSIC 2010	0.01	22	-	96	95	96	4	96	95
			21	+	95	94	95	5	95	94
		0.05	21	-	95	93	94	5	94	93
			21	+	94	92	92	6	93	92
		0.1	21	-	94	91	92	6	92	91
			20	+	93	90	92	7	91	90
	Enron Dataset	0.01	19	-	96	96	96	4	97	97
			19	+	95	95	95	5	96	95
		0.05	18	-	94	94	94	6	95	95
			17	+	95	93	93	5	94	95
		0.1	17	-	92	93	92	8	94	94
			16	+	92	92	91	8	93	93

Относительно проведенных исследований были сделаны следующие выводы:

1. Применение методов оптимизации атрибутов у аномальных запросов методом множественного анализа соответствий (глава 2) незначительно влияет на общую эффективность обучения и дальнейшего тестирования адаптивных алгоритмов. Таким образом, можно заключить, что использование данного метода имеет смысл с целью дальнейшей оптимизации ресурсов.
2. Эффективность классификатора на основе предложенной ИИС с использованием механизма анализа соответствий выше алгоритма логистической регрессии (не менее чем на 5%) и алгоритма на основе ИНС (не менее чем на 4%) в части точности и характеристики *F*-меры.
3. Выбранные алгоритмы эффективны при работе с разными наборами данных, что говорит об их универсальности и возможности применения в рамках любого протокола передачи данных, где требуется процесс бинарной классификации данных (мультипротокольность).
4. Меньшее количество атрибутов в запросе конкретного протокола увеличивает уровень ложных срабатываний в силу снижения чувствительности обучающего компонента адаптивного алгоритма.

Выводы о качестве классификации и анализе параметров алгоритмом ИИС:

1. Анализ набора данных ИИС показал, что, чем меньше аффинное расстояние, тем выше эффективность распознавания.

2. Общее количество β^m-элементов в среднем варьируется в диапазоне около 10-15% от количества β-элементов.

Дополнительно была произведена интеграция СОВ в корпоративную сеть с локальной сетевой инфраструктурой. Анализируемые протоколы: *HTTP1.1* и *SMTP*. Полученные запросы приводились к виду, эквивалентному виду запросов в множествах *CSIC 2010* (обучающая выборка: 15618; тестовая выборка: 4786) и *Enron Dataset* (обучающая выборка: 2375; тестовая выборка: 1755) соответственно.

Результаты применения СОВ с обозначенными адаптивными алгоритмами представлены в [Таблица 11].

Таблица 11 – Результаты работы классификаторов на основе алгоритма логистической регрессии (ЛР), ИНС и ИИС

		Оптимизация атрибутов			C_0(%)	C_1(%)	R_{TP}(%)	R_{FP}(%)	P(%)	F(%)
ЛР	СОВ1	-			86	79	87	14	89	90
		+			84	77	86	16	84	87
	СОВ2	-			86	90	91	14	89	91
		+			82	89	89	18	86	90
ИНС	СОВ1	-			88	79	87	12	89	90
		+			87	77	86	13	84	87
	СОВ2	-			87	91	91	13	89	91
		+			86	90	89	14	86	90
		Aff	β^m/β (%)	**Оптимизация атрибутов**	C_0(%)	C_1(%)	R_{TP}(%)	R_{FP}(%)	P(%)	F(%)
ИИС	СОВ1	0.01	22	-	97	96	96	3	92	95
			22	+	96	94	94	4	91	93
		0.05	19	-	95	94	93	5	90	93
			18	+	95	92	91	5	88	91
		0.1	16	-	94	91	90	6	88	91
			15	+	94	90	88	6	87	90
	СОВ2	0.01	21	-	94	93	94	6	92	93
			20	+	94	92	93	6	91	92
		0.05	20	-	93	91	92	7	90	91
			20	+	92	90	90	8	89	90
		0.1	19	-	92	89	90	8	89	89
			18	+	91	88	89	9	87	88

Анализ полученных результатов показал, что расчеты, полученные в результате применения СОВ в корпоративной сети, целиком и полностью согласуются с результатами, полученными при работе с *Dataset*'ами.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ РАБОТЫ И ВЫВОДЫ

1. Проведено исследование классов угроз, стадий их реализации, а также методов их обнаружения в рамках систем обнаружения вторжений, формулирование требований к адаптивным алгоритмам с целью обнаружения аномальных запросов.

2. Разработан метод оптимизации количества атрибутов в запросах, с помощью механизма анализа соответствий и вероятностных методов с получением репрезентативного набора данных для алгоритмов машинного обучения, позволяющий снизить количество анализируемых атрибутов не менее чем в 1,56 раза для эталонных наборов данных протоколов *TCP*, *HTTP/1.1* и *SMTP* и не менее чем в 2 раза для формируемых наборов данных.

3. Разработан метод кластеризации аномальных запросов с представлением атрибутов в номинальных шкалах, позволяющий снизить их количество для анализируемого множества в среднем не менее чем в 2.7 раза для эталонных наборов данных протоколов *TCP*, *HTTP/1.1* и *SMTP*.

4. Разработан алгоритм ИИС по обнаружению аномальных запросов для протоколов *TCP*, *HTTP/1.1* и *SMTP*, позволяющий повысить эффективность обнаружения угроз, по сравнению с алгоритмом логистической регрессии не менее чем на 5% и алгоритмом искусственной нейроной сети не менее чем на 4%, и уровнем ложного срабатывания не более 6% .

5. Разработан программный комплекс системы обнаружения вторжений для детектирования аномальных запросов, в основе которого лежат предложенные методы и алгоритмы. Результаты работы позволяют повысить надежность процесса классификации угроз, возникающих при генерации запросов к системе через протоколы передачи информации *TCP/UDP/ICMP*, *HTTP*/1.1 и *SMTP*.

Перспективы дальнейшей разработки. В рамках дальнейших исследований планируется применение разработанных методик и алгоритмов для повышения эффективности процесса обнаружения аномальных запросов. Реализация более эффективной СОВ с использованием в качестве базового компонента адаптивной защиты алгоритма искусственной иммунной системы.

СПИСОК ПУБЛИКАЦИЙ ПО ТЕМЕ ДИССЕРТАЦИИ

В рецензируемых журналах из списка ВАК

1. Бурлаков, М.Е. Метод фильтрации входящего трафика на основе двухслойной рекуррентной нейронной сети [Текст] / М.Е. Бурлаков // Ползуновский вестник - Алтайский государственный технический университет им. И.И. Ползунова. - 2012. - №3/2. - С. 215-219.

2. Бурлаков, М.Е. Модель многослойной универсальной системы обнаружения вторжений [Текст] / М.Е. Бурлаков // Доклады Томского Государственного университета систем управления и радиоэлектроники. - Томск: ТУСУР, 2014. - С. 214-219.

3. Бурлаков, М.Е. Выделение верхнего и нижнего пределов энергии при распознавании объектов нейронной сетью с механизмом реакции на последовательности [Текст] / М.Е. Бурлаков // Известия Волгоградского

государственного технического университета. - Волгоград: ИУНЛ ВолГТУ, 2014. - №12(139). - С. 58-60.
4. Бурлаков, М.Е. Двухклассификационная искусственная иммунная система [Текст] / М.Е. Бурлаков // Вестник Самарского государственного университета. - Самара, 2014. - №7(118). - С. 207-221.
5. Бурлаков, М.Е. Адаптация наивного байесовского классификатора к механизму классификации электронных сообщений [Текст] / М.Е. Бурлаков, Д.А. Голубых, М.Н. Осипов // Инфокоммуникационные технологии. - Самара, 2016. - Том 14. - № 2. - С. 199-203.

В рецензируемых журналах из списка Scopus

6. Burlakov, M.E. Research the behavior of elements in artificial immune system for intrusion detection systems in information networks [Text] / M.E. Burlakov, M.N. Osipov // CEUR Workshop Proceedings, ITNT 2016. Information Technology and Nanotechnology. Vol-1638, 2016 - P. 895-901.

Свидетельство о государственной регистрации программы для ЭВМ:

7. Свидетельство государственной регистрации программы для ЭВМ №2013618955. Программа для ЭВМ ГрандИС / М. Е. Бурлаков. Зарегистрирована 09.10.2013 г. - М.: Роспатент, 2013.
8. Свидетельство государственной регистрации программы для ЭВМ №2014617066. Двухклассификационная искусственная иммунная система. / М.Е. Бурлаков, М.Н. Осипов. Зарегистрирована 10.07.2014 г. - М.: Роспатент.

В других изданиях

9. Бурлаков, М.Е. Теоретическое обоснование реакционной модели нейрона на бинарные последовательности [Текст] / М.Е. Бурлаков // Научная дискуссия: вопросы физики, математики: Материалы IX международной научно-практической конференции. - М., 2013. - С. 61 - 68.
10. Бурлаков, М.Е. Динамическая система на нейронах с реакцией на последовательности на примере распознавания изображений: демонстрация реализации [Текст] / М.Е. Бурлаков // Перспективы развития информационных технологий: сборник материалов XII Международной научно-практической конференции / Под общ. ред. С.С. Чернова. – Новосибирск: ООО агентство «СИБПРИНТ», 2013. – С. 215-219.
11. Бурлаков, М.Е. Аудит безопасности локальной вычислительной сети с помощью динамической системы на нейронах с реакцией на последовательности [Текст] / М.Е. Бурлаков, М.Н. Осипов // Материалы XIII Международной научно-практической конференции "ИБ-2013". - Таганрог: Изд-во ЮФУ, 2013. - С. 85-91.
12. Бурлаков, М.Е. Выделение верхнего и нижнего предела энергии при распознавании объектов нейронной сетью с механизмом реакции на последовательности [Текст] / М.Е. Бурлаков // Материалы 9-ой Всероссийской школы семинара аспирантов и молодых ученых "Акуальные проблемы науки и техники". - Уфа: УГАТУ, 2014. - Том 2 - С. 61-67.
13. Бурлаков, М.Е. Выделение верхнего и нижнего предела энергии при распознавании объектов нейронной сетью с механизмом реакции на

последовательности [Текст] / М.Е. Бурлаков // Актуальные проблемы науки и техники. Девятая Всероссийская зимняя школа-семинар аспирантов и молодых ученых. - Уфа: УГАТУ, 2014. - Том 1 - С. 55-59.
14. Бурлаков, М.Е. Обзор базовых алгоритмов искусственных иммунных систем на клонально-селективной теории [Текст] / М.Е. Бурлаков // Сборник статей Международной научно-рактической конференции "Приоритетные направления развития науки". - УФА: Аэтерна, 2014. - С. 185-192.
15. Бурлаков, М.Е. О некоторых моделях оптимизации искусственной нейронной сети генетическими алгоритмами [Текст] / М.Е. Бурлаков // Перспективные информационные технологии (ПИТ-2014): труды Международной научно-технической конференции. - Самара: Издательство Самарского научного центра РАН, 2014. - С. 99-105.
16. Бурлаков, М.Е. Оптимизация наивного байесовского классификатора для решения задач классификации СМС сообщений [Текст] / М.Е. Бурлаков // Перспективные информационные технологии (ПИТ-2016): труды Международной научно-технической конференции. - Самара: Издательство Самарского научного центра РАН, 2016. - С. 209-215.
17. Бурлаков, М.Е. Исследование зависимости элементов двуклассификационной искусственной иммунной системы для обнаружения вторжений [Текст] / М.Е. Бурлаков // Сборник материалов Международной конференции и молодежной школы "Информационные технологии и нанотехнологии". - Самара: ИСОИ, 2016 - С. 398-405.
18. Бурлаков, М.Е. Базовые принципы работы загрузчика конфигурация в многоуровневой системе обнаружения вторжений [Текст] / М.Е. Бурлаков // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления, 2016. - № 19 - С. 55-68.
19. Бурлаков, М.Е. Исследование динамики активности обнаружения угроз в мобильных операционных системах и программах обмена сообщениями [Текст] / М.Е. Бурлаков, Ю.В. Алейнов, Д.А. Голубых // Вестник ПНИПУ. Электротехника, информационные технологии, системы управления, 2017. - №21б - С. 141-151.

Диссертант  М.Е. Бурлаков