шифроблоков. Для последующих шифроблоков в той же датаграмме счетчик увеличивается на 1 для каждого последующего. Такая организация счетчиков приводит к тому, что значение счетчика никогда не повторяется два раза. 46-ти битное значение блока криптосчетчика управляет 128 битами AES последовательности по следующему алгоритму: 46 бит повторяются 3 раза, в итоге получается 138-битная последовательность, 10 первых бит которой отбрасываются. Полученные 128 бит информации подвергаются обработке AES алгоритма, в результате чего получается случайная шифропоследовательность, которая потом взаимодействует с блоками данных.

Использование стандарта шифрования AES позволяет повысить безопасность личной информации конечных пользователей. Стандарт AES использует 128-битовые ключи и имеет высокую скорость работы, кодируя за один цикл 128-битный блок.

**Литература**

1. Эксперт: Телекоммуникации вчера, сегодня, завтра. [Электронный ресурс]. — Режим доступа: http://rfcmd.ru/book_07/h5_5. — Дата доступа: 13.05.2016.

## МОДЕЛИ ИНТЕЛЛЕКТУАЛЬНЫХ СИСТЕМ ПОИСКА АНОМАЛИЙ В ЗАДАЧАХ ОБНАРУЖЕНИЯ ВТОРЖЕНИЙ

А.А. Левчук

Методы анализа, используемые в большинстве современных систем детектирования вторжений, направлены на обнаружение известных и формально описанных типов воздействий, но зачастую оказываются не в состоянии обнаружить модификации или новые типы аномалий, что делает их использование не всегда эффективным.

В работе была поставлена задача: на основе изучения алгоритмов поиска аномалий, спроектировать и реализовать отдельные элементы интеллектуальной системы на основе нейронных сетей для применения в задачах обнаружения вторжений.

Для решения задачи был предложены архитектурные решения обнаружения аномалий с использованием нейросетевых моделей. В исследованиях были получены 4 варианта нейросетей, спроектированных путём комбинирования рециркуляционных нейронных сетей и многослойных персептронов.

Чтобы оценить эффективность предложенного подхода обнаружения вторжений, был проведён ряд экспериментов. База данных KDD Cup 99 использовалась для обучения и тестирования нейросетевых моделей. В базе KDD-99 представлены 22 типа атак, разделенных на четыре основных категории: DoS, U2R, R2L и Probe. Наилучший результат распознавания аномалий разработанной системой был достигнут для атак класса DoS и Probe, несколько хуже определяются U2R и R2L.

Таким образом, в работе подтверждено, что модели нейронных сетей могут успешно применяться в задачах обнаружения вторжений. В ходе эксперимента проведён сравнительный анализ спроектированных систем на основе нейронных сетей. Для сравнения были использованы такие показатели эффективности, как доля обнаруженных атак, доля распознанных атак по каждому классу и число ложных срабатываний.

## РЕШЕНИЕ ЗАДАЧИ ЦЕЛЕРАСПРЕДЕЛЕНИЯ В ИНФОРМАЦИОННОЙ ПОДСИСТЕМЕ КОМПЛЕКСА СРЕДСТВ АВТОМАТИЗАЦИИ ЗЕНИТНОЙ РАКЕТНОЙ БРИГАДЫ С УЧЕТОМ КЛАССА ЦЕЛЕЙ

А.Ю. Липлянин, Е.И. Михненок, Е.И. Хижняк

В основе эффективного управления боевыми средствами системы войск противовоздушной обороны лежит качественное управление огневыми средствами, решаемое в управляемой подсистеме комплексов средств автоматизации. Одним из факторов успешного функционирования управляющей подсистемы является эффективное решение задачи целераспределения. В настоящее время в комплексах средств автоматизации зенитной ракетной бригады имеется совокупность решаемых задач, в которые входят задачи боевого управления. Одним из типов таких задач является задача распределения усилий между группами зенитных ракетных дивизионов и целераспределение между зенитными ракетными дивизионами. На сегодняшний день эффективность зенитной ракетной бригады оценивается математическим ожиданием количества уничтоженных целей, которая в свою очередь обладает достаточно низкой коррелированностью с действительными результатами боевых действий [1]. Поскольку целью зенитной ракетной бригады при отражении удара воздушного противника является минимизировать ущерб объекту обороны, то и в качестве показателя