1. ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ Қ.И.Сәтбаев атындағы ҚазҰТУ-дың 80-жылдығы және Халықаралық ақпараттандыру академиясының 20 жылдығына арналған «ҚАЗАҚСТАНДАҒЫ АҚПАРАТТАНДЫРУДЫҢ ЖАҒДАЙЫ, МӘСЕЛЕЛЕРІ ЖӘНЕ МІНДЕТТЕРІ», Үшінші Халықаралық ғылыми-тәжірибелік конференциясының еңбектерінің жинағы, І-бөлім, 20-22 қараша 2014 жыл, Алматы қаласы

Б.С. Омаров, А.У.Актаева, Ш.Ж. Рамазанова «Нейрожелілік технология: ақпараттық ресурстарға жасалатын желілік шабуылдарды анықтаудағы фильтрлеу есебі.»

МИНИСТЕРСТВО
ОБРАЗОВАНИЯ И НАУКИ
РЕСПУБЛИКИ КАЗАХСТАН

Қ.И.Сәтбаев атындағы ҚазҰТУ-дың 80 жылдығы және
Халықаралық ақпараттандыру академиясының 20 жылдығына арналған

«ҚАЗАХСТАНДАҒЫ АҚПАРАТТАНДЫРУДЫҢ ЖАҒДАЙЫ, МӘСЕЛЕЛЕРІ ЖӘНЕ МІНДЕТТЕРІ»

Үшінші Халықаралық ғылыми-тәжірибелік конференциясының
ЕҢБЕКТЕРІНІҢ ЖИНАҒЫ
I БӨЛІМ
20-22 қараша 2014 жыл
Алматы қ.

СБОРНИК ТРУДОВ
Третьей Международной научно-практической конференции

«СОСТОЯНИЕ, ПРОБЛЕМЫ И ЗАДАЧИ ИНФОРМАТИЗАЦИИ В КАЗАХСТАНЕ»

посвященной 80-летию КазНТУ им. К.И.Сатпаева
и 20-летию Международной Академии Информатизации

ЧАСТЬ I
20-22 ноября 2014 года
г. Алматы

WORKS BOOK
of the Third International scientifically-practical conference

«STATUS, PROBLEMS AND CHALLENGES OF INFORMATIZATION IN KAZAKHSTAN»

Dedicated to the 80 anniversary of KazNTU named after K. I. Satpayev
and to the 20 anniversary of the International informatization academy

PART I
20-22 of November 2014
ALMATY c.

УДК 004 (574) (063)
ББК 32.81
С 66

С 66 **Состояние, проблемы и задачи информатизации в Казахстане** Сборник трудов Третьей Международной конференции. г. Алматы, 20-22 ноября 2014 г. – Алматы: КазНТУ; МАИН, 2014. – Ч.1 – 275 с.

ISBN 978-601-228-662-5
ISBN 978-601-228-663-2

В первую часть сборника включены доклады и научные статьи, представленные на Третьей Международной научно-практической конференции «Состояние, проблемы и задачи информатизации в Казахстане», посвященной 80-летию КазНТУ имени К.И. Сатпаева и 20-летию МАИН.

Материалы могут быть полезны для специалистов, работающих в различных сферах информатизации, а также преподавателям высших учебных заведений, докторантам, магистрантам и студентам.

Дизайн – Васько Т.В.

ISBN 978-601-228-663-2 (ч.1)
ISBN 978-601-228-662-5 (общ.)

НЕЙРОЖЕЛІЛІК ТЕХНОЛОГИЯ: АҚПАРАТТЫҚ РЕСУРСТАРҒА ЖАСАЛАТЫН ЖЕЛІЛІК ШАБУЫЛДАРДЫ АНЫҚТАУДАҒЫ ФИЛЬТРЛЕУ ЕСЕБІ

Б.С. Омаров, А.У.Актаева, Ш.Ж. Рамазанова
Қазақстан, Әл- Фараби атындағы Қазақ ұлттық университеті, bauyrzhan_os@mail.ru

Қазіргі уақытта компьютерлік желілірді қорғаудың жасанды нейронды желіге (ЖНЖ) және статистикалық анализге негізделген түрлі технологияларының көптеген түрлері жасалынып жатыр. Желілік шабуылдарды табу бұл классификация жүргізуге болатындай белгілердің үлкен санының бөлінуіне байланысты.

Белгілер ақпараттық тең мағыналы емес, сонымен қатар олардың нақты мәндерін қосымша зерттеулер жүргізулерден соң ғана анықтауға болады.

Желілік шабуылдарды фильтрлеу есебі. Есеп жалпы нормадан ауытқыған желілік белсенділік мониторингының нейрожелілік технология негізіндегі шабуылдарды табуға арналған нейрожелілік тәсілдер мен программалық жабдықтауларды өңдеуде тұжырымдалады. Шабуылдарды екі тәсілмен табуға болады[1]:

- *Сигнатуралық тәсіл* әлдеқашан белгілі шабуылдардың белгілерін іздеуге бағытталған. Сигнатуралық тәсілдің артықшылығы – ол іс жүзінде жалған жарамсыздықтарға ұшырамайды. Бұл тәсілдің кемшілігі жүйеге алынбаған шабуылдарды анықтау мүмкін еместігі болып табылады.
- *Ауытқуларды (аномалия) іздеу тәсілі* алдын-ала белгісіз шабуылдарға әрекет етуге мүмкіндік береді, бірақ жалған жарамсыздықтарға ұшырайды және әрбір бақыланған объект үшін нақты күйге келтіруді талап етеді.

Нейрожелілік жүйелерді оқыту және шабуылдарды бейнелеу есептерін қосу келесі сұлбада ұсынылады (1-сурет.):

(1) ақпараттық белгілерді іздеу және алу,

(2) белгілерді БКӘ немесе РНЖ көмегімен сығымдау[2],

(3) екі қабатты персептрон мен белгіленген ақпараттық векторлар базасындағы Кохонен желісінің белгілерін үйрету.