артықшылықтары туралы түсінік беріледі және сымсыз байланыстың өзгеріп отыратын қажеттіліктерін қанағаттандыру үшін үнемі жаңашылдықтың қажеттілігін көрсетеді.

**АЛҒЫС**

Бұл жариялым Erasmus+ ACeSYRI «Компьютерлік ғылымдар саласындағы докторанттар мен жас зерттеушілерге арналған озық орталық» жобасын іске асыру нәтижесі, тіркеу нөмері 610166-EPP-1-2019-1-SK-EPPKA2-CBHE-JP.

УДК 004.056.5
МРНТИ 81.93.29

**Бапиев Идеят Мэлсович,** Ph.D, https://orcid.org/0000-0001-8468-8938
НАО «Западно-Казахстанский аграрно-технический университет имени Жангир хана», г. Уральск, ул. Жангир хана 51, 090009, ЗКО, Казахстан, bapiev@mail.ru
**Искакова Молдир Ержанкызы,** учитель информатики, педагог-исследователь, https://orcid.org/0000-0002-4920-4798
ГККП "Сырымский колледж" управления образования акимата ЗКО, Сырымский район, с. Жымпиты, ул. Жумагалиева 18, 090009, ЗКО, Казахстан, moldir.iskakova99@mail.ru
**Bapiyev Ideyat**, Ph.D. https://orcid.org/0000-0001-8468-8938
Zhangir Khan West Kazakhstan Agrarian-Technical University, Uralsk, Zhangir Khan's st., 51, 090009, West Kazakhstan region, Kazakhstan, bapiev@mail.ru
**Iskakova Moldir Yerzhankyzy**, teacher of ICT, teacher-researcher , https://orcid.org/0000-0002-4920-4798
SCCP "Syrym College" of the Department of Education of the Akimat of the West Kazakhstan region, Syrymsky district, Zhympity village, Zhumagalieva str. 18, 090009, West Kazakhstan region, Kazakhstan, moldir.iskakova99@mail.ru

## НЕЙРОСЕТЕВЫЕ МОДЕЛИ ОЦЕНКИ ПАРАМЕТРОВ БЕЗОПАСНОСТИ ИНТЕРНЕТ МАГАЗИНОВ
## NEURAL NETWORK MODELS FOR EVALUATING THE SECURITY PARAMETERS OF ONLINE STORES

**АННОТАЦИЯ**

Серьезной проблемой для бизнеса является опасность взлома интернет магазина. После взлома работа сайта цифровой коммерции прекращается. Современное состояние интернет магазинов, интегрированных в глобальную сеть, характеризуется повышенным уровнем требований к безопасности информации, который уже сложно обеспечить с помощью систем защиты информации, в подсистемах контроля и управления которых используются исключительно классические методы оценивания параметров безопасности. Вместе с тем, в различных областях науки и техники проявляется интерес к использованию методов теории искусственных нейронных сетей. Популярность искусственных можно объяснить эффективностью их применения в задачах классификации и кластеризации образов, аппроксимации функций, прогнозирования, оптимизации, управления, создания информационно-вычислительных систем с ассоциативной памятью, которые частично или в комплексе необходимо решать при оценке параметров безопасности для выявления кибератак. Чтобы обеспечить защиту интернет магазинов от кибератак мы предлагаем анализировать входящие и исходящие данные сетевого трафика с помощью нейронных сетей для обнаружения аномалий. Нейронные сети используются для распознавания кибератак в межсетевых экранах компании Cisco и для распознавания вирусов в антивирусах Norton Antivirus производства компаний Symantec, F-Prot и CYREN GlobalView Security Lab. Также с помощью НС определяются DDOS-атаки в свободно распространенном модуле, предназначенном для интегрирования в программный комплекс Snort. Технологии киберпреступников не стоят на месте. Многие хакеры нацеливаются именно на сферу электронной коммерции, ведь именно сюда вливаются колоссальные инвестиции.

***Ключевые слова**: интернет магазины, кибератаки, нейроные сети.*

**Введение**. Базой для анализа современных нейросетевых моделей и методов, применяемых в системах защиты интернет магазинов, стали работы [1-17]. В большинстве проанализированных работ есть определенное несоответствие терминологического аспекта описанной разработки: нейросетевой метод, модель, система, технология, средство. Как правило, приводится комплексное описание разработки, хотя название работы указывает, например, на создание нейросетевой модели. Поэтому анализ этих работ проведен с единых позиций определения основных характеристик и методов нейросетевых моделей. Приведем полученные данные.

Методы простой и семантической классификации сетевых атак. Методы разработаны в рамках нейросетевой технологии обнаружения сетевых компьютерных атак с помощью программного комплекса «Snort», описанной в работе [26]. Технология предусматривает применение двух нейросетевых методов обнаружения атак – простой классификации (ПСК) и семантической классификации (ССК). В качестве входных параметров используются параметры сетевых пакетов транспортного уровня стека протоколов TCP/IP. В методе ПСК использован многослойный персептрон с 10 входными нейронами и 2 нейронами в выходном слое. Для оптимизации количества скрытых нейронов предлагается применение конструктивных алгоритмов. Приведены выражение для расчета коррекции весовых коэффициентов нейронов выходного слоя:

$$\Delta w_{jk}(i) = -\eta(y_n(i) - f(x_i))\varphi'(v_n(i))y_n, \quad (1)$$

где $\eta$ – коэффициент скорости обучения; $n$ – номер нейрона в выходном слое; $i$ – номер учебной итерации; $v_n$ – информационное поле, полученное на входе функции активации; $y_n$ – выходной сигнал $n$-го выходного нейрона; $\varphi'$ – производная функции активации; $f(x_i)$ – желаемый отклик $i$-го нейрона.

Отметим отсутствие детального описания процесса оптимизации структуры многослойного персептрона. В методе ССК предлагается использование топографической карты Кохонена, выбор которой обосновывается ее невысокой ресурсоемкостью. В обоих методах предусмотрена обработка входных параметров с целью уменьшения количества входных параметров нейронной сети.

Метод нейросетевой фильтрации спама приведен в работе [28], в которой доказывается оптимальность использования аддитивных нейронных сетей. Вид нейросетевой модели выбран с позиций максимизации точности распознавания, возможности автоматизации обучения и возможности представления результатов в графическом виде. То есть использовано процедуру многокритериальной оптимизации процесса определения архитектуры нейронной сети. В качестве входных параметров нейросетевой модели использованы частоты встречи в спаме и в целевых электронных письмах информативных слов. Также предложена процедура многокритериальной оптимизации параметров нейронной сети, в которой использованы критерии максимизации вычислительной мощности и минимизации срока обучения.

**Материалы и методы исследования.** Метод определения фрагментов программного кода описан в работе [27]. Этот метод применяется для определения перечня и оценки значений входных параметров нейронной сети, используемых в системах детектирования вредоносного программного обеспечения. Также в работе [18] приведены описание и результаты экспериментов по распознаванию вредоносного программного обеспечения, проведенных с помощью многослойного персептрона. Анализ приведенных результатов подтверждает перспективность предложенного метода. Можно сделать вывод об использовании в методе процедуры предварительной обработки входных параметров нейронной сети, которая повышает их информативность.

Нейросетевая система обнаружения вторжений на интернет магазины описана в работе [19]. Эта система ориентирована на использование многослойного персептрона для распознавания сетевых атак. Приведены результаты экспериментов, подтверждающие эффективность системы при распознавании атак, сигнатуры которых представлены в базе

KDD-99. Выбор типа нейронной сети обоснован с позиций максимальной вычислительной мощности. Также проведена однокритериальная оптимизация архитектуры многослойного персептрона.

Нейросетевой подход выявления SQL-инъекций представлен работе [20]. Предложено рассматривать проблему определения вредоносных SQL-запросов в виде проблемы прогнозирования временных рядов. Предлагается использовать рекуррентные НС типа Джордана и Элмана. То есть тип нейронной сети выбран в соответствии с критерием апробированности в задачах прогнозирования временных рядов. Также приведены процедура предварительной обработки входных параметров и процедура однокритериальной оптимизации структуры нейронной сети. Использован критерий максимизации вычислительной мощности. Приведенные результаты экспериментальных исследований, проведенные на основе данных портала Php-Nuke, подтверждают перспективность предложенного подхода.

Бинарный нейросетевой метод описан в работе [21]. Этот метод применяется для решения задачи обнаружения сетевых атак на интернет магазины. В основе метода лежит специальная бинарная нейронная сеть, которая имеет два важных свойства. Во-первых, модель приспособлена для решения задач, в которых входная информация имеет сложную, многосвязную и даже фрактальную структуру. Во-вторых, метод обучения модели является прямой вычислительной процедурой и не сводится к поиску глобального экстремума сложной нелинейной функции, что не накладывает никаких принципиальных ограничений на размерность задачи. Таким образом, в методе предусмотрен выбор вида нейросетевой модели по критерию апробированности в задачах определенного типа и по критерию минимизации длительности обучения. К сожалению, в работе отсутствуют экспериментальные данные, что затрудняет сравнительный анализ. В методе не предусмотрено проводить оптимизацию структуры нейронной сети, применения и процедуры обработки входных данных.

Метод обнаружения сетевых атак с типичного сетевого трафика описан в работе [22]. Этот метод применяется для распознавания сетевых атак. Предложено применение многослойного персептрона с 2 скрытыми слоями нейтронов. Входной слой такого многослойного персептрона состоит из девяти нейронов, а выходной слой – с одного нейрона. Отмечено, что выбор многослойного персептрона с такой структурой объясняется требованиями гибкости и функциональности. То есть использовано многокритериальную оптимизацию структуры нейронной сети. Указано на предварительную обработку статистики, используемой для учебной и тестовой выборки.

Способ обнаружения DDoS-атак на интернет магазины приведен в работе [23]. Предложено использование нечетких нейронных сетей. Предложение основывается на перспективности НМ такого типа; акценттируется на распознавании DDoS-атаки типа SYN Flood. Для формализации знаний экспертов о DDoS-атаки было создано пять лингвистических переменных, каждая из которых характеризует одну из компонент вектора параметров сетевого трафика, используемого для формирования входных параметров нейронной сети. К указанным лингвистическим переменным относятся: $X_1$ – время получения пакетов; $X_2$ – процент пакетов из различных внешних *ip*-адресов; $X_3$ – процент пакетов с разных портов; $X_4$ – процент пакетов с поврежденными заголовками; $S$ – степень уверенности. Разработаны предикатные правила вида: Если $X_1 =$ «большой» $\rightarrow Y \rightarrow$ «высокий». Предложено представить нечеткий классификатор в виде НС с прямым распространением сигнала, который учится с помощью модифицированного алгоритма обратного распространения ошибки. Модификация заключается в приспособлении классического алгоритма к нечетким нейронам «И» и «ИЛИ». Таким образом, основным отличием описанного способа является возможность применения для обучения НС экспертных знаний.

**Результаты исследования.** Базовые характеристики проанализированных нейросетевых методов и моделей приведены в табл. 1. Анализ данных этой таблицы указывает на то, что большинство известных нейросетевых моделей предназначены для распознавания сетевых атак. При этом в качестве базовых видов нейросетевых моделей используются многослойные персептроны и топографические карты.

Кроме того, в результате проведенного анализа установлено, что обеспечение эффективности современных нейросетевых методов и моделей идет путем обеспечения в них определенных возможностей, которые характеризуются с помощью следующих критериев: $\phi_{\text{по}}$

– предварительная обработка входных параметров; $ф_{ота}$ – однокритериальная оптимизация вида архитектуры; $ф_{мва}$ – многокритериальная оптимизация вида архитектуры; $ф_{опа}$– однокритериальная оптимизация параметров архитектуры; $ф_{мпа}$ – многокритериальная оптимизация параметров архитектуры; $ф_{омо}$ – оптимизация метода обучения; $ф_{иэп}$ – возможность использования экспертных правил.

Приведенный перечень дополнен критериями $ф_{мна}$ и $ф_{одв}$, указывающими на возможность применения в методе классических и перспективных видов нейросетевых моделей, а также возможность принципиальной оценки целесообразности применения нейронных сетей для решения поставленной задачи. Основой использования параметра $ф_{мна}$ является приведенное в работах [24, 25] утверждение о том, что в системах защиты информации, как и в большинстве известных приложений, развитие нейросетевых методов и моделей идет путем приспособления базовых и перспективных нейросетевых архитектур к условиям поставленных практических задач. Основой использования параметра $ф_{одв}$ является объективная необходимость четко очерченной области применений нейронной сети в системах защиты интернет магазинов.

Величины предложенных критериев в первом приближении можно оценить так: критерий равен –1, когда соответствующая возможность в нейросетевом методе или модели не обеспечивается, 0 – когда обеспечивается опосредованно и 1 – когда обеспечивается непосредственно.

Таблица 1- Базовые характеристики нейросетевых методов и моделей

| № | Метод | Распознавание | | | | | Тип НС | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | ВПО | Атак на БД | Спам | Сетевых атак | МСП | КН | ТК | НСДЭ | АНС | ННС | БНМ | РНМ | Все типы |
| 1 | ОФПК | + | - | - | - | + | - | - | - | - | - | - | - | - |
| 2 | МКН | | | | | - | + | - | - | - | - | - | - | - |
| 3 | МТК | | | | | - | - | + | - | - | - | - | - | - |
| 4 | НИИС | | | | | | | | | | | | | |
| 5 | НВПИ | - | + | - | - | - | - | - | + | - | - | - | - | - |
| 6 | ОНДБД | | | | | + | - | - | - | - | - | - | - | - |
| 7 | НФС | - | - | + | - | - | - | - | - | + | - | - | - | - |

Для проанализированных случаев величины определения критериев приведены в табл. 2. При этом для всех проанализированных методов значение критериев $ф_{мна}$= $ф_{одв}$ =–1. Только для АППТ $ф_{мна}$= 1, а $ф_{одв}$= 0.

То есть в большинстве методов нельзя использовать весь перечень классических и перспективных видов НСМ и ни в одном из методов (моделей) не предусмотрена оценка принципиальной целесообразности его применения. Также отметим, что базовый перечень параметров может быть в дальнейшем расширен. Практическая ценность данных табл. 2 заключается в определении недостатков и перспектив совершенствования современных нейросетевых методов и моделей. Например, величины $ф_{по}$=0, $ф_{бва}$=–1 свидетельствуют о том, что к недостаткам метода НСОВ можно отнести недостаточную оптимизацию вида НСМ. Это свидетельствует о возможности соответствующего совершенствования указанного метода. При этом ни один из рассмотренных методов не предполагает полноценной оптимизации НСМ, согласно с условиями поставленной задачи и полноценного использования в такой модели экспертных правил.

Таблица 2 - Величины критериев, характеризующих нейросетевые методы и модели

| № п/п | Модель, метод | Параметр | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | $ф_{по}$ | $ф_{ота}$ | $ф_{бва}$ | $ф_{опа}$ | $ф_{бпа}$ | $ф_{омн}$ | $ф_{веп}$ | $ф_{мна}$ | $ф_{одв}$ |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
| 1 | ОФПК | 1 | 0 | -1 | 0 | -1 | 0 | 1 | -1 | -1 |
| 2 | МКН | 1 | 1 | -1 | -1 | -1 | -1 | -1 | -1 | -1 |

| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 |
|---|---|---|---|---|---|---|---|---|---|---|
| 3 | МТК | 1 | 1 | -1 | 0 | -1 | -1 | -1 | -1 | -1 |
| 4 | НИИС | -1 | 1 | -1 | 1 | -1 | -1 | -1 | -1 | -1 |
| 5 | НВПИ | 1 | 1 | 0 | 0 | -1 | 0 | -1 | -1 | -1 |
| 6 | ОНДБД | 1 | 0 | -1 | 0 | -1 | -1 | -1 | -1 | -1 |
| 7 | НФС | 1 | 1 | 0 | 1 | 0 | 1 | -1 | -1 | -1 |

В результате проведенного анализа видно, что в современных системах обнаружения атак на интернет магазины в основном используются классические виды нейросетевых моделей, которые в той или иной степени адаптированы к условиям поставленной задачи.

**Заключение.** Проанализировав результаты исследования можно сделать вывод о том, что важным и актуальным направлением повышения эффективности систем распознавания кибератак на ресурсы интернет магазинов является применение нейросетевых моделей, методов и средств оценивания параметров безопасности. Несмотря на определенные достижения в этой области, эффективному применению таких средств мешают такие недостатки:

– недостаточная оперативность реагирования на новые виды кибератак;

– недостаточная адаптация к вариативности условий применения и действия при ограниченных вычислительных ресурсах;

– недостаточная точность распознавания кибератак;

– недостаточная взаимосвязь известных нейросетевых подходов, моделей и методов оценки пб для выявления кибератак;

– отсутствие нейросетевых средств, которые на основе комплексной нейросетевой методологии позволят решать наиболее актуальные задачи распознавания кибератак на интернет магазины.

Для исправления этих недостатков определены два направления научных исследований:

1. Развитие теоретического базиса нейросетевого оценивания параметров безопасности интернет магазинов.

2. Применение разработанных теоретических положений для последовательного создания нейросетевых моделей, методов и систем оценки параметров безопасности интернет магазинов.

Решение второго направления исследований связано с комплексной переработкой моделей, методов и систем, которые основаны на предложенных теоретических решениях и учитывают особенности современных видов кибератак.

## СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Айтчанов Б.Х., Бапиев И.М. Разработка процедуры определения ожидаемого выходного сигнала нейросетевой модели распознавания кибератак // Международный журнал прикладных и фундаментальных исследований. – М., Академия естествознания, – 2017г., – Ч. 1, – № 5, – С. 8 - 11

2. Аль-Мехди С.Т, Евланенкова О. Применение нейронных сетей для обнаружения вторжений // Доклады ТУСУР. – 2014. – №4. – С. 28-33.

3. Ахметов Б.Б., Корченко А.Г., Терейковский И.А. Параметры оценки эффективности нейросетевых средств распознавания кибератак на сетевые ресурсы информационных систем // Reports of the national academy of sciences of the republic of Kazakhstan. ISSN 2224-5227. Volume 2, Number 312 (2017)

4. Бапиев И.М., Ахметов Б.С., Корченко А.Г. Применение нейронной сети с радиальными базисными функциями для распознавания скриптовых вирусов // II международная научно-практическая конференция «Актуальные вопросы обеспечения кибербезопасности и защиты информации». – Киев: Европейский университет, 24-27 февраль 2016, С. 21-24.

5. Бапиев И.М., Корченко А.Г., Терейковский И.А. Разработка критериев оценки эффективности нейросетевых средств распознавания кибератак на сетевые ресурсы информационных систем // IV International scientific conference «Global and regional problems of informatizition in society and nature using». – Kyiv: National University of Life and Environmental Sciences of Ukraine, 23-24 of June 2016, P. 80-82.

6. Бапиев И.М. Правила для определения эффективных видов нейросетевых моделей распознавания кибератак на сетевые ресурсы // III Международная научно-практическая конференция «Актуальные вопросы обеспечения кибербезопасности и защиты информации». – Киев: Европейский университет, 22-25 февраль 2017, С. 27-30.

7. Безобразов С.В., Головко В.А. Алгоритмы искусственных имунных систем и нейронных сетей для обнаружения вредоносных программ // Нейроинформатика. – 2010. – №7. – С. 273-288.

8. Беляев А. Петренко С. Системы обнаружения аномалий: новые идеи в защите информации // Экспресс-Электроника. – 2004. – № 2. – С. 12–14.

9. Большев А.К. Алгоритмы преобразования и классификации трафика для обнаружения вторжений в компьютерные сети: авторефер. … канд. техн. наук: 05.13.19 – Методы и системы защиты информации, информационная безопасность. – Санкт-Петербург, 2011. – 36 с.

10. Браницкий А.А. Котенко И.В. Обнаружение сетевых атак на основе комплексирования нейронных, иммунных и нейронечетких классификаторов // Информационно-управляющие системы. – 2015. – №3. С. 69-77.

11. Васильев В.И., Хафизов А.Ф. Нейронные сети при обнаружении атак в сети Internet (на примере атаки SYNFLOOD) // Нейрокомпьютеры в информационных и экспертных системах. – М.: Радиотехника, 2007. – №6. – С. 34-38.

12. Вилков А.С. Информационная безопасность персональных ЭВМ и мониторинг компьютерных сетей. – М.: МИНИТ ФСБ России, 2005. – 210 с.

13. Галушкин А.И. Теория нейронных сетей. – М.: ИПРЖР, 2000. – 416 с.

14. Горбань А.Н., Россиев Д.А. Нейронные сети на персональном компьютере. – Новосибирск: Наука, 1996. – 276 с.

15. Гришин А.В. Нейросетевые технологии в задачах обнаружения компьютерных атак // Информационные технологии и вычислительные системы. – 2011. – №1. – С. 53 -64.

16. Ежов А.А., Шумский С.А. Нейрокомпьютинг и его применения в экономике и бизнесе. – М.: МИФИ, 1998. – 224 с.

17. Емельянова Ю.Г., Талалаев А.А., Тищенко И.П. Нейросетевая технология обнаружения сетевых атак на информационные ресурсы // Программные системы: теория и приложения. – 2011. – №3(7). – С. 3–15.

18. Жульков Е. Поиск уязвимостей в современных системах IDS // Открытые системы. – 2003. – № 7–8. – С. 16–18.

19. Заенцев И.В. Нейронные сети: основные модели. – Воронеж: Воронежский гос. ун-т, 1999. – 76 с.

20. Закер К. Компьютерные сети / пер. с англ. – СПб.: БХВ-Петербург, 2000. – 1008 с.

21. Зима В.М., Молдовян А.А., Молдовян Н.А. Безопасность глобальных сетевых технологий. – СПб.: БХВ-Петербург, 2000. – 450 с.

22. Каллан Р. Основные концепции нейронных сетей / пер. с англ.; под ред. А.Г. Сивака. – М.: Вильямс, 2003. – 288 с.

23. Касперски К. Техника и философия хакерских атак. – М.: Солон, 2001. – 256 с.

24. Кузнецов Г.В., Иванов А.М. Методы анализа данных для обнаружения атак в компьтерных сетях банковских структур // Защита информации: Сб. науч. трудов. – К.: НАУ, 2004. – С. 45–50.

25. Лукацкий А.В. Обнаружение атак. – СПб.: БХВ-Петербург, 2003. – 624 с.

26. Люгер Ф. Искусственный интеллект: стратегии и методы решения сложных проблем, 4-е издание / пер. с англ.; под ред. Н.И. Галагана. – М.: Вильямс, 2003. – 864 с.

27. Магницкий Ю.Н. Использование бинарной нейронной сети для обнаружения атак на ресурсы распределенных информационных систем // Динамика неоднородных систем. – 2008. – С. 200-205.

28. Мустафаев А.Г. Нейросетевая система обнаружения компьютерных атак на основе анализа сетевого трафика [Электронный ресурс] // Вопросы безопасности. - 2016. - № 2. - С.1-7. DOI: 10.7256/2409-7543.2016.2.18834. URL: http://e-notabene.ru/nb/article_18834.html (дата обращения: 19.03.2023)

**БЛАГОДАРНОСТЬ**

Эта публикация является результатом реализации проекта Erasmus+ «Передовой центр для докторантов и молодых исследователей в области информатики» (ACeSYRI), регистрационный номер 610166-EPP-1-2019-1-SK-EPPKA2-CBHE-JP.

ӘОЖ 004.3

**Касымова Акмарал Хамзиевна**, педагогика ғылымдарының кандидаты, https://orcid.org/0000-0002-4614-4021
«Жәңгір хан атындағы Батыс Қазақстан аграрлық-техникалық университеті» КеАҚ, Орал қ., Жәңгір хан көшесі 51, 090009, Қазақстан
**Канашов Батыржан Адилханович**, магистрант, https://orcid.org/0000-0001-5054-5277, «Жәңгір хан атындағы Батыс Қазақстан аграрлық-техникалық университеті» КеАҚ, Орал қ., Жәңгір хан көшесі 51, 090009, Қазақстан, b.kanashov@mail.ru

# МОБИЛЬДІ ҚОСЫМШАЛАРДЫ ЖӘНЕ ОЛАРДЫ ӘЗІРЛЕУ ҚҰРАЛДАРЫН САЛЫСТЫРМАЛЫ ТАЛДАУ
# MOBILE APPLICATIONS AND THEIR DEVELOPMENT COMPARATIVE ANALYSIS OF TOOLS

**ТҮЙІН**

Мақалада, қазіргі уақыттағы мобильді құрылғыларға арналған қосымшаларды әзірлеуге арналған ақпараттық технологиялар белсенді дамып келетіндігі және мобильді қосымшаларды қолдану аймағы және құрылымы тұрғысынан жіктеу қарастырылған. Мобильді қосымшаларды құрудың кейбір құралдары талданады, оларды қолдану мысалдары келтірілген. Мобильді қосымшаларды әзірлеудің негізгі кезеңдері қарастырылған. Білім алушыларға мобильді әзірлеу тұтынушылардың қалауын болжай алатын қолданбаларды жасауға бағытталған; есептерді шешу, шешу алгоритмі алдын ала белгісіз. Енді қолданбалар бірнеше көздерден алынған ақпаратты аналитикалық талдауды жүзеге асыра алады және пайдаланушыға шешім қабылдауға, процестерді басқаруға және басқа маңызды міндеттерді өзі үшін ең аз уақыт пен аналитикалық шығындармен шешуге көмектеседі. Оқу орындарына арналған мобильді қосымшаларды пайдалану мүмкіндіктерін білімалушылрға бірыңғай бақылауды жүзеге асыру; сынақтар мен сынақтарды жеңілдету; білім беру процесінің барлық қатысушылары арасында ақпарат алмасуды жеделдету, мұғалімдер мен студенттердің өзара әрекеттесу процесін жеңілдету; оқу-тәрбие процесін жандандыру және жаңарту; қашықтықтан білім беру үшін мобильді құрылғыны пайдалану ұсынылады.

**ANNOTATION**

The article discusses the fact that information technologies for developing applications for mobile devices are currently actively developing, and the classification of mobile applications in terms of application area and structure is considered. Some tools for creating mobile applications are analyzed, examples of their use are given. The main stages of mobile application development are considered. Mobile development for students is aimed at creating applications that can predict consumer preferences; the algorithm for solving, solving problems is unknown in advance. Now applications can carry out analytical analysis of information from several sources and help the user make decisions, manage processes and solve other important tasks with minimal time and analytical costs for himself. Implementation of unified control over students of the possibilities of using mobile applications for educational institutions; simplification of tests and tests; acceleration of information exchange between all participants in the educational process, simplification of the process of interaction between teachers and students; activation and updating of the educational process; for distance education, it is recommended to use a mobile device.