МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ
ДОНЕЦКОЙ НАРОДНОЙ РЕСПУБЛИКИ

ИНФОРМАТИКА И КИБЕРНЕТИКА

2 (12)

Донецк – 2018

УДК 004.3+004.9+004.2+51.7+519.6+519.7

ИНФОРМАТИКА И КИБЕРНЕТИКА, № 2 (12), 2018,
Донецк, ДонНТУ.

Представлены материалы по вопросам приоритетных направлений научно-технического обеспечения в области информатики, кибернетики и вычислительной техники.

Материалы предназначены для специалистов народного хозяйства, ученых, преподавателей, аспирантов и студентов высших учебных заведений.

Рекомендовано к печати ученым советом ГОУ ВПО «Донецкий национальный технический университет» Министерства образования и науки ДНР. Протокол № 5 от 22 июня 2018 г.

Электронное периодическое издание «Научный журнал «Информатика и кибернетика» зарегистрирован в Министерстве информации ДНР.
Свидетельство о регистрации: серия ААА № 000145 от 20.06.2017.

Контактный адрес редакции
ДонНТУ, ул. Артема, 58, Донецк, 83001
Тел.: +380 (62) 301-08-56. Эл. почта: infcyb.donntu@yandex.ru
Интернет: http://infcyb.donntu.org

СОДЕРЖАНИЕ

Компьютерные и информационные науки

Информатика и вычислительная техника

Инженерное образование

Компьютерные и информационные науки

УДК 512.579

О многообразиях альтернативно определённых тернарных полугрупп

А. В. Решетников
Национальный исследовательский университет «Московский институт электронной техники», г. Москва
a_reshetnikov@hush.com

Решетников А. В. О многообразиях альтернативно определённых тернарных полугрупп. *Рассматриваются альтернативно определённые тернарные полугруппы G с операцией f, то есть тернарные гурппоиды, удовлетворяющие тождеству $f(f(x, a, b), y, z) = f(x, f(b, y, a), z) = f(x, y, f(a, b, z))$. Для нетривиальных G доказано следующее. Если G идемпотентна и любая её 2-порождённая подполугруппа абелева, то G содержит двухэлементную альтернативно определённую тернарную подполугруппу; если G не идемпотентна, то она содержит в качестве подполугруппы либо двухэлементную 3-полугруппу с константным умножением, либо конечную циклическую 3-группу, либо бесконечную циклическую 3-полугруппу. Аналогичные результаты в бинарном случае были получены Калицким Я. и Скоттом Д. в 1955 г. и применены к описанию атомов решётки многообразий полугрупп.*

Ключевые слова: *n-арная альтернативность, абелева n-арная полугруппа, атомы решётки многообразий, альтернативная ассоциативность.*

Постановка задачи

Пусть f — n-арная операция, заданная на некотором множестве G. Тогда G называется *n-арным группоидом с операцией f* и обозначается через (G, f). n-арная операция f *ассоциативна*, если при любых значениях i, j, удовлетворяющих неравенствам $1 \le i, j \le n$, для неё справедливо тождество

$$f(x_1,..., x_{i-1}, f(x_i, \dots, x_{i+n-1}), x_{i+n}, \dots, x_{2n-1}) = f(x_1,..., x_{j-1}, f(x_j, \dots, x_{j+n-1}), x_{j+n}, \dots, x_{2n-1}).$$

n-арной полугруппой называется n-арный группоид с ассоциативной операцией. Бинарную полугруппу будем называть *полугруппой*.

Мы полагаем [1], что существует глубокая связь между полугруппами и универсальными алгебрами, удовлетворяющими тождеству

$$f(f(x, u, v), y, z) = f(x, f(v, y, u), z) = f(x, y, f(u, v, z)). \quad (1)$$

Условие (1) мы называем *альтернативным тождеством ассоциативности*, а универсальные алгебры с таким тождеством — *альтернативно определёнными тернарными полугруппами*.

Пусть S_n – группа подстановок на множестве $\{1, ..., n\}$. Для произвольной n-арной операции f и подстановки $\sigma \in S_n$ введём обозначение:

$$f^\sigma(x_1, ..., x_n) = f(x_{\sigma(1)}, ..., x_{\sigma(n)}).$$

Нетрудно доказать следующее утверждение.

Теорема 1. Если тернарная операция f удовлетворяет тождествам (1), то для любой подстановки $\sigma \in S_3$ операция f^σ также удовлетворяет тождествам (1).

Данная теорема переносит известный в теории полугрупп принцип двойственности на альтернативно определённые тернарные полугруппы и таким образом связывает бинарную ассоциативность с альтернативной тернарной ассоциативностью. Для классических (то есть не альтернативно определённых) тернарных полугрупп легко указать пример, когда утверждение, аналогичное теореме 1, неверно (подробнее см. [1]).

Коль скоро бинарные полугруппы и альтернативно определённые тернарные полугруппы схожи, было бы интересно сравнить решётки их многообразий. В то время как атомы решётки многообразий классических n-арных полугрупп полностью описаны [2] для любого n, удовлетворительное описание атомов решётки многообразий альтернативно определённых тернарных полугрупп не известно.

В статье [3] авторам для описания атомов решётки многообразий бинарных полугрупп потребовалось утверждение, которое на современном языке общей алгебры можно сформулировать следующим образом:

Предложение 2. Любая *полугруппа S, состоящая хотя бы из двух элементов, содержит в качестве подполугруппы либо двухэлементную полугруппу, либо циклическую группу простого порядка, либо бесконечную циклическую полугруппу, а именно:*

1) если каждый элемент полугруппы S *является идемпотентом, то:*

1.1) если S — коммутативная *полугруппа, то для любых двух различных элементов $x, y \in S$ либо $\{x, y\}$ (в случае $xy = x$), либо $\{x, xy\}$ (в случае $xy \ne x$) — двухэлементная полурешётка;*

1.2) если существуют *такие элементы* $x, y \in S$, *что* $xy \neq yx$, *то либо* $\{xyx, yx\}$ — *двухэлементная полугруппа левых нулей, либо* $\{xy, yx\}$ — *двухэлементная полугруппа правых нулей (если* $xyx = yx$*);*

2) если элемент $x \in S$ *не* является *идемпотентом, то:*

2.1) если циклическая полугруппа $\langle x \rangle$, *порождённая элементом x, имеет период длины 1, то* $\{x^{k-1}, x^k\}$ — *полугруппа с нулевым умножением, где* $x, x^2, \ldots, x^k$ *различны и* $x^k = x^{k+1} = x^{k+2} = \ldots$

2.2) если $\langle x \rangle$ *имеет конечный период Y, длина которого превышает 1, то существует подмножество множества Y, элементы которого образуют циклическую группу простого порядка;*

2.3) в противном случае $\langle x \rangle$ — *бесконечная циклическая полугруппа.*

Приведём для альтернативно *определённых* тернарных полугруппах известные на данный момент утверждения, схожие в той или иной мере с предложением 2.

Пусть G — n-арный группоид с *операцией* f. Подмножество $G' \subseteq G$ назовём его *подгруппоидом*, если G' — n-арный группоид с операцией f', определяемой следующим условием:

$f'(x_1, \ldots, x_n) = f(x_1, \ldots, x_n)$ для всех $x_1, \ldots, x_n \in G'$.

Пересечение всех *подгруппоидов* n-арного группоида G, которые содержат некоторое подмножество $X \subseteq G$, назовём *n-арным группоидом, порождённым множеством X*. Подгруппоид, порождённый одноэлементным множеством, назовём *циклическим*. n-арную полугруппу S будем называть *циклической*, если само множество S является её циклическим подгруппоидом. Определение циклической n-арной группы см., например, в монографии [4].

Лемма 3. Пусть G — *альтернативно определённая тернарная полугруппа с операцией f, удовлетворяющая тождествам*

$$f(x, x, y) = f(x, y, x) = f(y, x, x);$$

$$f(x, x, x) = x. \qquad (3)$$

Если $|G| \geq 2$, *то G содержит в качестве подгруппоида альтернативно определённую тернарную полугруппу, а именно:*

1) если существуют элементы $x, y \in G$ *такие, что* $f(x, y, y) = y$ *и* $f(y, y, x) = x$, *то подгруппоид, порождённый множеством* $\{x, y\}$, *изоморфен альтернативно определённой тернарной полугруппе на множестве* $\{0, 1\}$ *с операцией сложения по модулю 2;*

2) в противном случае существуют элементы $x, y \in G$ *такие, что* $f(x, y, y) \neq y$, *и то подгруппоид, порождённый множеством* $\{f(x, y, y), y\}$, *изоморфен альтернативно определённой тернарной полугруппе на множестве* $\{0, 1\}$ *с операцией умножения по модулю 2.*

Пусть f — n-арная операция, заданная на некотором множестве S. Будем говорить, что S — *n-арная полугруппа с константным умножением*, если

$$f(x_1, \ldots, x_n) = f(y_1, \ldots, y_n)$$

для всех $x_1, \ldots, x_n, y_1, \ldots, y_n \in G$.

Лемма 4. *Пусть G — альтернативно определённая тернарная полугруппа с операцией f, удовлетворяющая тождеству (2) и не удовлетворяющая тождеству (3). Тогда G содержит в качестве подгруппоида либо бесконечную циклическую полугруппу, либо циклическую тернарную группу, либо двухэлементную тернарную полугруппу с константным умножением.*

Отметим также следующую теорему, которая в вопросе об описании атомов решётки многообразий альтернативно определённых тернарных полугрупп дополняет лемму 4:

Теорема 5 [4, теорема 2.5.54]. *Конечная n-арная группа G не имеет собственных n-арных подгрупп тогда и только тогда, когда она циклическая и множество простых делителей числа $|G|$ является подмножеством множества простых делителей числа* $(n - 1)$.

Литература

1. Решетников А. В. Об альтернативном определении тернарной полугруппы // Сборник научных трудов МИЭТ. Посвящается 70-летию профессора А. С. Поспелова. 2016. С. 110—116.

2. Артамонов В. А. Минимальные многообразия обобщенных полугрупп, групп и колец // Сибирский математический журнал. 1980. Т. 21. №3. С. 6—22.

3. Kalicki J., Scott D. Equational completeness in abstract algebras // Indagationes Mathematicae. 1955. Vol. 17. P. 650—659. Русский перевод: Калицкий Я., Скотт Д. Эквациональная полнота абстрактных алгебр // Кибернетический сборник: сб. переводов. [Вып.] 2 / Под ред. А. П. Ершова [и др.; пер. А. Воскресенский и др.]. М.: Изд-во иностранной литературы, 1961. С. 41—52.

4. Гальмак А. М. n-Арные группы. Ч. I. Гомель: ГГУ им. Ф. Скорины, 2003. 196 с.

Решетников А. В. О многообразиях альтернативно определённых тернарных полугрупп. *Рассматриваются альтернативно определённые тернарные полугруппы G с операцией f, то есть тернарные гурппоиды, удовлетворяющие тождеству f(f(x, a, b), y, z) = f(x, f(b, y, a), z) = f(x, y, f(a, b, z)). Для нетривиальных G доказано следующее. Если G идемпотентна и любая её 2-порождённая подполугруппа абелева, то G содержит двухэлементную альтернативно определённую тернарную подполугруппу; если G не идемпотентна, то она содержит в качестве подполугруппы либо двухэлементную 3-полугруппу с константным умножением, либо конечную циклическую 3-группу, либо бесконечную циклическую 3-полугруппу. Аналогичные результаты в бинарном случае были получены Калицким Я. и Скоттом Д. в 1955 г. и применены к описанию атомов решётки многообразий полугрупп.*

Ключевые слова*: n-арная альтернативность, абелева n-арная полугруппа, атомы решётки многообразий, альтернативная ассоциативность.*

Reshetnikov A. V. On varieties of alternatively determined ternary semigroups *In this paper we consider the alternatively defined semigroups G with operation f, i.e. the ternary groupoids satisfying the identity f(f(x, a, b), y, z) = f(x, f(b, y, a), z) = f(x, y, f(a, b, z)). For the non-trivial G the following assertions are proved. If G is idempotent and every its 2-generated subsemigroup is abelian, then G contains a two-element alternatively defined subsemigroup; if G is not idempotent, then there is a subsemigroup of G which is either two-element 3-semigroup with constant multiplication, or a finite cyclic 3-group, or an infinite cyclic 3-semigroup. Similar results were obtained by Kalicki J. and Scott D. in 1955 and applied to describe the atoms of the lattice of semigroup varieties.*

Keywords*: n-ary alternativity, abelian n-ary semigroup, atoms of lattice of varieties, alternative associativity.*

Статья поступила в редакцию 23 мая 2018 г.
Рекомендована к публикации профессором Шелеповым В. Ю.

УДК 514.1124

Три задачи по геометрии на тему: «Разделение треугольника на части с заданными свойствами»

В. А. Свентковский
Московский автомобильно-дорожный государственный технический университет, г. Москва
vladimirsventkovskiy@gmail

Свентковский В. А. Три задачи по геометрии на тему: «Разделение треугольника на части с заданными свойствами». *Приводится доказательство того, что треугольник с рациональными сторонами можно разбить на 2 треугольника с рациональными сторонами неограниченным числом способов. Строится соответствующий алгоритм. Дается четкий алгоритм разделения треугольника на 9 выпуклых пятиугольников. Доказывается, что тупоугольный или прямоугольный треугольник разделяется на остроугольные треугольники. Строится соответствующий алгоритм.*

Ключевые слова: *треугольник, пятиугольник, части, рациональные стороны, заданные свойства.*

Введение

Доказывается, что на границе треугольника с рациональными сторонами найдется неограниченное число точек, все три расстояния от которых до вершин также рациональны. Аналогичный вопрос для точек внутри треугольника с рациональными сторонами остался пока для автора открытым. На этот вопрос может пролить свет компьютерный эксперимент в дальнейшем.

Существует, как известно, три типа треугольников, в зависимости от их углов: остроугольные, прямоугольные и тупоугольные.

Автор ставит естественный вопрос, (который средней школой не рассматривается) – можно ли треугольник любого из перечисленных трех типов разделить на треугольники любого из этих трех типов?

Очевидно, любой треугольник проведением высоты из большего угла делится на 2 прямоугольных треугольника.

Ясно также, что проведением трех средних линий любой треугольник делится на 4 подобных, равных треугольника того же типа.

Ясно также, что любой треугольник делится на три тупоугольных треугольника, при соединении точки пересечения его биссектрис с вершинами треугольника.

Остался не рассмотренным уже не столь простой вопрос о разделении тупоугольного или прямоугольного треугольника на остроугольные треугольники. Положительный ответ на него доказывается в теореме 2.

Причем это доказательство доступно для продвинутого школьника.

Далее, если поставить вопрос, на какие выпуклые k-угольники можно разбить треугольник, то для k=3 найти решение может любой школьник.

Для к=4 – не любой, а для k=5 лишь некоторые. Четкий алгоритм автора (теорема 3), позволяет большинству школьников (да и взрослых) научиться быстро решать задачу для k=5. Для K>5 не удалось найти в литературе рассмотрения этого вопроса (или хотя бы упоминания), хотя сам вопрос естественно приходил в голову разным математикам. Отсюда автор делает вывод, что, наверное, этот вопрос пока не получил ответа. Хотя, возможно, при K>5 треугольник и нельзя разрезать на выпуклые K-угольники.

Теорема 1

Любой треугольник с рациональными сторонами можно разбить на два треугольника с рациональными сторонами.

Доказательство

Доказательство основано на том факте, что любое рациональное положительное число может быть представлено как разность квадратов двух различных рациональных чисел. Этот факт ниже доказывается.

Пусть задан произвольный треугольник ABC с рациональными сторонами (рис. 1).

Пусть

$$AB=c,\ BC=a,\ AC=b, \qquad (1)$$

где a,b,c- рациональные числа; BH-высота треугольника ABC;

AC-большая сторона.

Достаточно доказать, что на стороне AC найдется точка D, такая, что длины отрезков AD, BD- рациональны (так как, если AH-рационально, то

$$DC=AC-AD \qquad (2)$$

– тоже рационально).

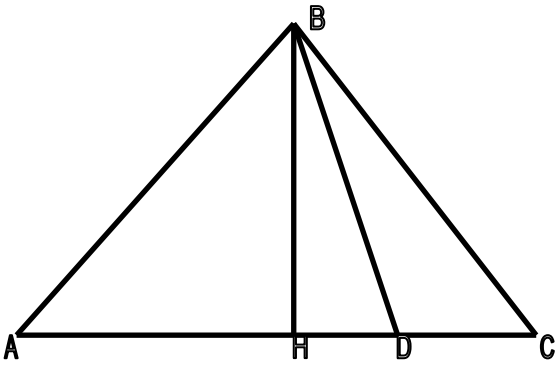


Рисунок 1 – Треугольник с рациональными сторонами

Из теоремы косинусов следует, что

$$a^2 = b^2 + c^2 - 2bc\cos A,\ \cos A = \frac{b^2 + c^2 - a^2}{2bc}. \qquad (3)$$

Отсюда следует, что косинусы углов A,B,C – рациональны. Поэтому

$$AH = c\cos A = \frac{b^2 + c^2 - a^2}{2b} = R \qquad (4)$$

- рационально.

Пусть

$$BD = x,\ \ HD = y. \qquad (5)$$

Тогда

$$BH^2 = AB^2 - AH^2 = c^2 - R^2 = r = x^2 - y^2 = (x+y)(x-y) \qquad (6)$$

Итак,

$$(x+y)(x-y) = r. \qquad (7)$$

Пусть

$$x - y = t. \qquad (8)$$

Тогда

$$x + y = \frac{r}{t}. \qquad (9)$$

Из (8), (9) следует

$$x = \frac{t + r/t}{2}; y = \frac{r/t - t}{2}. \qquad (10)$$

Задавая рациональное t, получаем рациональные x, y.

Достаточно найти такое рациональное t, чтобы выполнились неравенства

$$h < \frac{t + r/t}{2} < a \qquad (11)$$

Построим график (рис. 2):

$$x = \frac{t + r/t}{2}. \qquad (12)$$

Асимптоты:

$$t = 0; x = t/2.\ x' = 0.5\left(1 - r/t^2\right), \qquad (13)$$

$$t_0 = \sqrt{r}. \qquad (14)$$

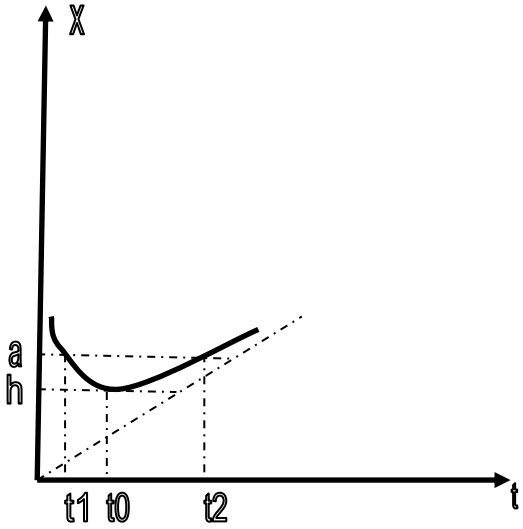


Рисунок 2 – График функции $x = \frac{t + r/t}{2}$

Найдем t_1, t_2:

$$\frac{t + r/t}{2} = a, \qquad (15)$$

$$t^2 - 2at + r = 0.$$

$$t_{1,2} = \frac{2a \pm \sqrt{4a^2 - 4r}}{2} = a \pm \sqrt{a^2 - r}, \qquad (16)$$

$$t_1 = a - \sqrt{a^2 - r},\ t_2 = a + \sqrt{a^2 - r}. \qquad (17)$$

Выбирая любое рациональное число $t \in (t_1, t_0)$, (а таких чисел бесконечное множество), получаем по формулам (10) рациональные x, y. Если точку D искать на отрезке AH, то точке D соответствует число t_1. Если же точку D искать на отрезке HC, то точке D соответствует число t_2.

Пусть теперь вершина B проектируется не на сторону AC, а на ее продолжение, то есть угол A или C – тупой (рис. 3).

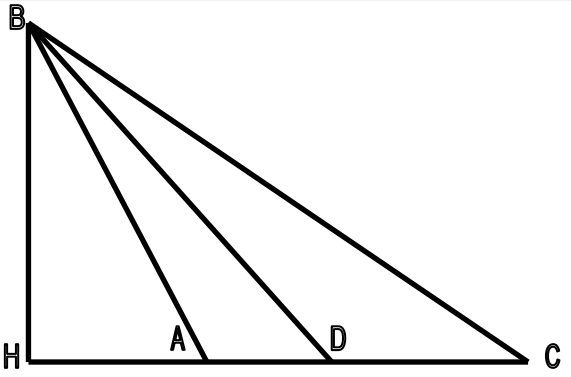


Рисунок 3 – Треугольник с тупыми углами A и C

В этом случае

$$AH=-cosA \qquad (18)$$

- рационально.

Поэтому CH- рационально, а, значит,

$$BH^2 = BC^2 - CH^2 \qquad (19)$$

- рационально.

Теперь, если положить

$$BD = x, HD = y, \qquad (20)$$

то рассуждения повторяются,

$$BH^2 = AB^2 - AH^2 = c^2 - R^2 = r = x^2 - y^2 = (x+y)(x-y) = r \qquad (21)$$

Итак,

$$(x+y)(x-y) = r. \qquad (22)$$

Пусть

$$x - y = t. \qquad (23)$$

Тогда

$$x + y = \frac{r}{t}. \qquad (24)$$

Из (23), (24) следует

$$x = \frac{t + r/t}{2}; y = \frac{r/t - t}{2}. \qquad (25)$$

Задавая рациональное t, получаем рациональные x, y.

Достаточно найти такое рациональное t, чтобы выполнились неравенства

$$c < \frac{t + r/t}{2} < a. \qquad (26)$$

Построим график (рис. 4):

$$x = \frac{t + r/t}{2}. \qquad (27)$$

Асимптоты:

$$t = 0; x = t/2. \qquad (28)$$

Имеем:

$$x' = 0.5\left(1 - r/t^2\right).$$

$$x'' = 0.5\left(\frac{2r}{t^3}\right) = \frac{r}{t^3} > 0. \qquad (29)$$

Поэтому график имеет следующий вид:

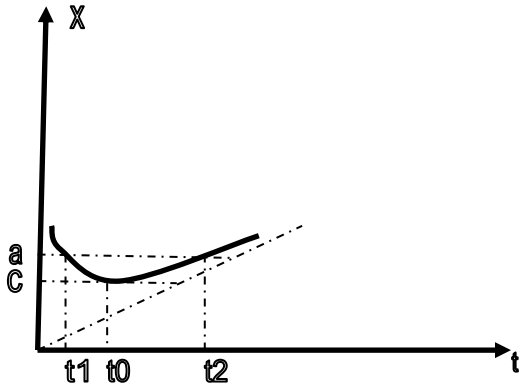


Рисунок 4 – График функции $x = \frac{t + r/t}{2}$

Имеем:

$$t_0 = \sqrt{r}. \qquad (30)$$

Найдем t_1, t_2:

$$\frac{t + r/t}{2} = a;\ t^2 - 2at + r = 0 \qquad (31)$$

$$t_1 = a - \sqrt{a^2 - r},\ t_2 = a + \sqrt{a^2 - r}. \qquad (32)$$

Выбирая любое рациональное число

$$t \in (t_0, t_2), \qquad (33)$$

(а таких чисел бесконечное множество), получаем по формулам (10) рациональные x, y. Если точку D искать на отрезке AH, то точке D соответствует число t_1. Если же точку D искать на отрезке HC, то точке D соответствует число t_2.

Теорема 1 доказана.

Выводы

На границе треугольника содержится всюду плотное множество точек, для которых все три расстояния от вершин – рациональные числа. Интересно, есть ли не только на границе, но и внутри любого треугольника с рациональными сторонами, подобное множество троек рациональных расстояний до вершин треугольника? Шансов для этого меньше, поскольку для точек внутри треугольника из условия, что одно расстояние от вершины – рационально, не следует, что оба других расстояний от вершин – рациональны.

Более того, пока неясно, всегда ли внутри любого треугольника с рациональными сторонами найдется хотя бы одна точка с тремя рациональными расстояниями до вершин треугольника. Компьютерный эксперимент должен обнаружить упомянутое всюду плотное множество, если оно существует. Промоделировать ситуацию можно на первом треугольнике с различными минимальными целыми сторонами: 2,4,5.

Теорема 2

Любой равнобедренный тупоугольный или прямоугольный треугольник можно разделить на 7 остроугольных треугольников. Любой неравнобедренный тупоугольный треугольник делится на 14 остроугольных треугольников.

Доказательство

Лемма 1

Равнобедренный тупоугольный или прямоугольный треугольник можно разделить на семь остроугольных треугольников (рис. 5, 6).

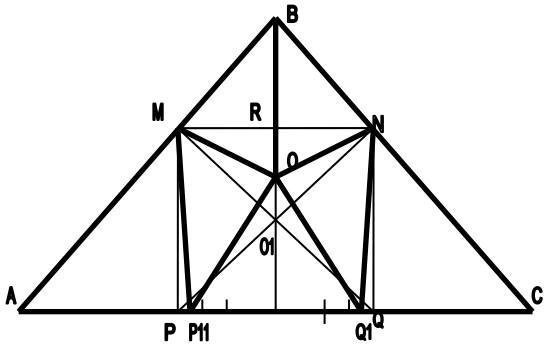


Рисунок 5 – Деление равнобедренного тупоугольного треугольника на семь остроугольных (вариант 1)

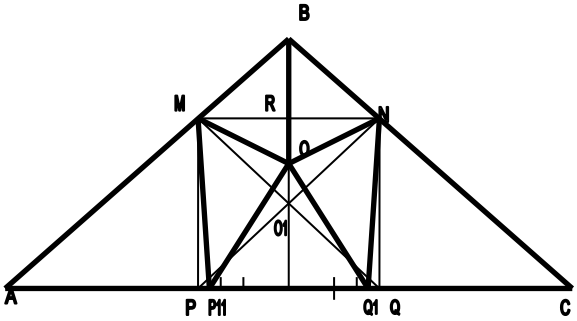


Рисунок 6 – Деление равнобедренного тупоугольного треугольника на семь остроугольных (вариант 2)

Рассмотрим равнобедренный тупоугольный треугольник ABC.

Угол B- тупой

$$\angle B > 90^0 \qquad (34)$$

Пусть

$$AC=b,\ BD=h. \qquad (35)$$

Пусть MNPQ- квадрат, вписанный в треугольник ABC. Пусть сторона квадрата MN равна *a*. Тогда из подобия треугольников следует

$$\frac{a}{b}=\frac{h-a}{h}. \qquad (36)$$

Отсюда

$$ah=bh-ab.\ a=\frac{bh}{b+h}. \qquad (37)$$

Отрезок "*a*" строится на основе теоремы Фалеса с помощью отложения отрезков *h, b+h, h* на сторонах угла и проведения: *SF||VU* (рис. 7).

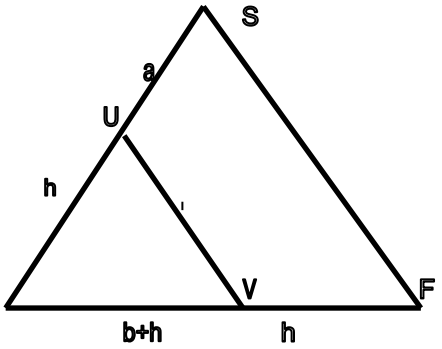


Рисунок 7 – Иллюстрация теоремы Фалеса

Если центр квадрата соединить с его вершинами, то получим 4 равнобедренных прямоугольных треугольника, составляющих квадрат, два прямоугольных треугольника: AMP, CNQ.

Тогда

$$\angle MBR=\frac{\angle B}{2}>\frac{90^0}{2}=45^0,$$

$$\angle BMR<45^0, \qquad . \qquad (38)$$

$$\angle RMO1=\angle MO1Q=45^0$$

В треугольнике O1MB

$$\angle O1MB<45^0+45^0=90^0 \qquad (39)$$

Треугольник MBO1- остроугольный, треугольник NO1B тоже остроугольный. Возьмем произвольную точку O внутри отрезка RO1, например в его середине. Теперь соединим ее с вершинами квадрата. Тогда пятиугольник MBNPQ разбился на пять треугольников: MBO, NBO, POQ, MOP, QON (рис. 8). Все эти пять треугольников - остроугольные.

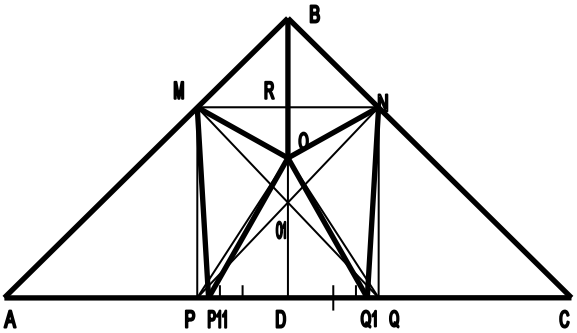


Рисунок 8 – Разбиение пятиугольника MBNPQ на пять треугольников

Осталось еще два прямоугольных треугольника: AMP, CNQ. Их можно превратить в остроугольные, "чуть" сместив вершины Q и P в сторону вершины D.

При этом остроугольные треугольники немного деформируются, но останутся остроугольными по непрерывности при достаточно малом смещении.

Докажем это.

Пусть

$$QQ1=PP1=ka \quad (40)$$

Нужно показать, что углы MQ1O, MOQ1- острые, при достаточно малом положительном k.

Пусть

$$k=1/16=0.125/2=0.0625. \quad (41)$$

Применим теорему косинусов.

$$c1^2 = a^2 + (0.0625a)^2 = 1\frac{1}{256}a^2;$$

$$MO^2 = (a/2)^2 + (a/4)^2 = \frac{5}{16}a^2 \quad (42)$$

$$OP1^2 = (a/2 - a/16)^2 + (a - a/4)^2 =$$

$$= (7a/16)^2 + (3a/4)^2 =$$

$$= (49/256 + 9/16)a^2 =$$

$$= \frac{49+144}{256}a^2 = \frac{193}{256}a^2 \quad (43)$$

$$MP1^2 = a^2 + (0.0625a)^2 =$$

$$= 1\frac{1}{256}a^2 \quad . \quad (44)$$

Отсюда

$$OM < OP! < MP1. \quad (45)$$

Наибольший угол против большей стороны MQ1 – это угол MOQ1.

$$\cos\angle MOP1 = \frac{MO^2 + OP1^2 - MP1^2}{2MO \cdot OP1} =$$

$$= \frac{5/16 + 193/256 - 257/256}{2 \cdot MO \cdot OP1} = \quad . \quad (46)$$

$$= \frac{80-63}{2MO \cdot OP1} > 0$$

Угол MOP1 - острый. Остальные два угла треугольника MOP1- еще меньше, поэтому тоже острые.

Теперь, если (вдруг) оказалось, что AM<AP1, то сдвигаем точку Q1 влево так, чтобы стало

$$AP1=AM. \quad (47)$$

Тогда треугольник AMP1 становится равнобедренным с острым углом A при вершине. Поэтому этот треугольник – остроугольный.

Аналогичную операцию проводим с вершиной Q1.

Алгоритм деления построен.

Замечание

Если равнобедренный треугольник - прямоугольный, то доказательство того, что его можно разделить на 7 остроугольных треугольников, в точности повторяет доказательство для равнобедренного тупоугольного треугольника, с тем лишь отличием, что AP1<AM, и потому точку P1 сдвигать не надо. Действительно,

$$AM = a\sqrt{2} > AP1 = a + a/8 = 9a/8, \quad (48)$$

Так как

$$2 > 81/64. \quad (49)$$

Лемма 1 доказана.

Лемма 2

Любой неравнобедренный прямоугольный треугольник делится медианой, проведенной из вершины прямого угла на два треугольника: равнобедренный тупоугольный и равнобедренный остроугольный (рис. 9).

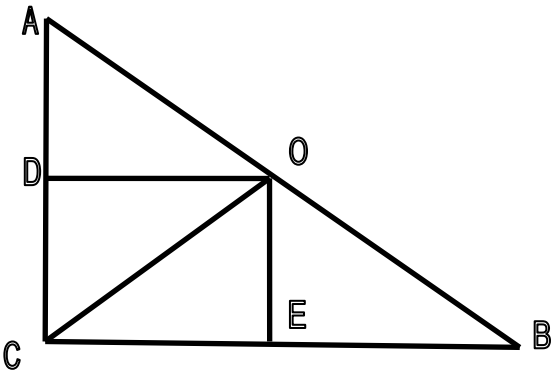


Рисунок 9 – Неравнобедренный прямоугольный треугольник

Действительно, проведя две средних линии и соединив точки C и O, получим 4 равных прямоугольных треугольника, гипотенузы которых равны. Поэтому AO=CO,CO=BO, треугольники AOC, COB- равнобедренные, причем один из них остроугольный. Поэтому второй – остроугольный.

Лемма 2 доказана.

Лемма 3

Любой треугольник делится на 2 прямоугольных треугольника.

Действительно, проведя из вершины против большей стороны высоту BH, получаются два прямоугольных треугольника ABH и CBH (рис. 10).

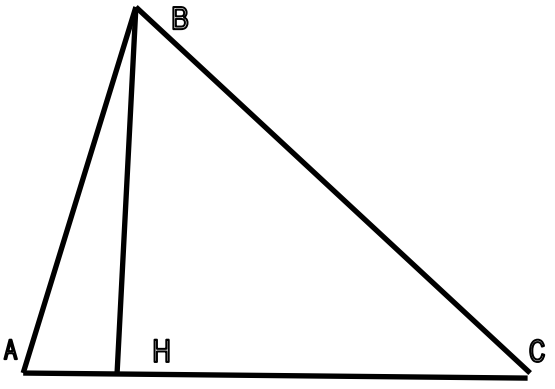


Рисунок 10 – Иллюстрация доказательства леммы 3

Лемма 3 доказана.

Из лемм 1,2,3 следует теорема 2. Теорема 2 доказана.

Теорема 3

Любой треугольник можно разделить на 9 выпуклых пятиугольников (рис. 11).

Доказательство

По определению, выпуклая фигура – такая, которая лежит целиком по одну сторону от любой своей стороны.

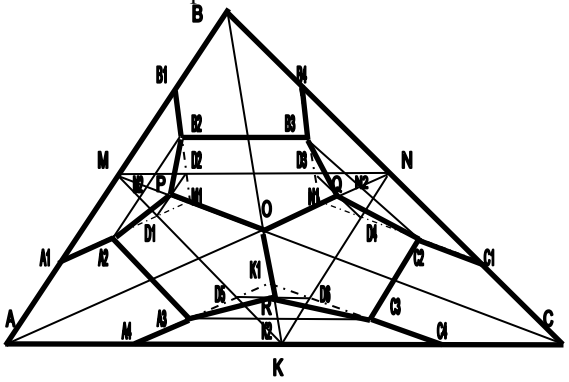


Рисунок 11 – Иллюстрация доказательства теоремы 3

Пусть AN,BK,CM-медианы треугольника ABC; MK, NK, MN—средние линии. Пусть A1-середина AM, M1- середина MO, поэтому A1M1||AO. Пусть B1-середина BM, A4- середина AK, K1-середина OK. Тогда A4K1||AO. Значит A1M1||A4K1.

Пусть C1 – середина CN, C4 – середина KC; K1 – середина OK, N1 – середина ON. Тогда K1C4||OC, N1C1||OC.

Пусть, $D2 = B1M1 \cap MN$; $P = MO \cap D1D2$. Тогда D1D2||AB.

Пусть A2- середина A1D1, B2-середина B1D2. Тогда A2B2||AB. Пятиугольник A1`A2PB2B1-выпуклый.

Пусть $D3 = MN \cap B4N1$, $D4 = C1N1 \cap ON$, $Q = ON \cap D3D4$. Пусть B3 – середина B4D3, C2- середина D4C1. Тогда пятиугольник B4B3QD4C2C1 – выпуклый.

Пусть $D5 = A4K1 \cap MK$, $D6 = K1C4 \cap NK$, $R = OK \cap D5D6$. Пусть A3-середина MD5, C3-середина C4D6. Тогда $K2 = K1K \cap A3A4$-середина RK. Пятиугольник MA3RC3C4– выпуклый.

Три угловых пятиугольника имеют по две равных параллельных стороны – выпуклые. Три пятиугольника с центром в точке O – тоже выпуклы.

Теорема доказана.

Замечание. Если выбросить обозначения вершин, то получается рисунок 12.

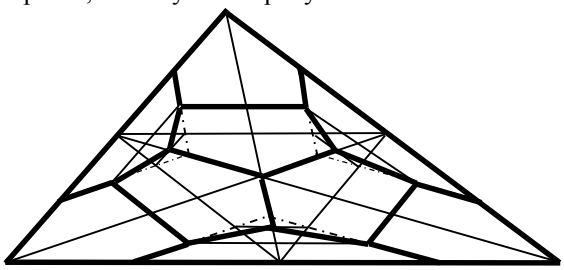


Рисунок 12 – Разделение на выпуклые пятиугольники без обозначения вершин

Литература

1. Свентковский В. А. Математика и ее приложения. Выпуск 1. “Некоторые задачи и проблемы комбинаторной геометрии”, Санкт Петербург, 2008.

2. Свентковский В. А. О построении плоских выпуклых K-угольников, которые можно разделить на n любых заданных равных прямоугольных треугольников. Сборник материалов VIII международной научно-технической конференции 25 мая 2017 ДонНТУ Донецк

3. Бухштаб А. А. Теория чисел. Санкт-Петербург. Изд-во Лань, 2015.

4. Чандрасекхаран К. Введение в аналитическую теорию чисел.

5. Манин Ю. И. Введение в современную теорию чисел. Москва. Издат-во МЦНМО, 2013.

6. Серпинский В. Пифагоровы треугольники. Учпедгиз - 1959.

7. Яглом И. М. О комбинаторной геометрии. Москва. Изд-во Едиториал, 2004.

8. Яглом И. М. Как разрезать квадрат? М: КомКнига, 2006.

9. Болтянский В. Г., Гохберг И. Ц. Разбиение фигур на меньшие части. Москва, Изд-во Наука, 1971.

10. Александро И. И. Сборник геометрических задач на построение. Москва, Учпедгиз, 1959.

11. Гордин Р., Шарыгин И. Сборник задач по геометрии. Изд-во “АСТ”, “Астрель”, 2001.

12. Шарыгин Г. И. Лекции по элементарной геометрии. Москва, Изд-во МЦНМО, 2014.

Свентковский В. А. Три задачи по геометрии на тему: «Разделение треугольника на части с заданными свойствами». *Приводится доказательство того, что треугольник с рациональными сторонами можно разбить на 2 треугольника с рациональными сторонами неограниченным числом способов. Строится соответствующий алгоритм. Дается четкий алгоритм разделения треугольника на 9 выпуклых пятиугольников. Доказывается, что тупоугольный или прямоугольный треугольник разделяется на остроугольные треугольники. Строится соответствующий алгоритм.*

Ключевые слова: *треугольник, пятиугольник, части, рациональные стороны, заданные свойства.*

Smentkowski V. A. Three problems on geometry on the theme: «Splitting a triangle into parts with desired properties». *The proof that a triangle with rational sides can be divided into 2 triangles with rational sides unlimited number of ways. Built matching algorithm. Provides a clear separation algorithm of the triangle is 9 convex pentagons. It is proved that obtuse or right triangle is divided into acute triangles. Built matching algorithm.*

Keywords: *triangle, pentagon, parts, the rational part, the desired properties.*

Статья поступила в редакцию 21 мая 2018 г.
Рекомендована к публикации профессором Шелеповым В. Ю.

Информатика и вычислительная техника

УДК 004.771

Беспроводная технология Wi-Fi. Уязвимости и методы защиты

В. И. Вязмин, А. В. Чернышова
Донецкий национальный технический университет
testerreality@gmail.com, chernyshova.alla@rambler.ru

Вязмин В. И., Чернышова А. В. Беспроводная технология Wi-Fi. Уязвимости и методы защиты. *В статье рассмотрены стандарты Wi-Fi, методы защиты и взлома беспроводных вычислительных сетей. Определены слабые стороны и подчеркнуты сильные стороны передачи данных с помощью технологии Wi-Fi.*

Ключевые слова: *Беспроводная вычислительная сеть, защита, атака, уязвимость, стандарт, данные.*

Стандарт Wi-Fi

В наше время наиболее развивающейся технологией, которая присутствует на большинстве устройств, является беспроводная локальная сеть (Wi-Fi), однако она как помогает, так и имеет множество уязвимостей. Wi-Fi [1] (происходит от английского сокращения Wireless Fidelity) – семейство протоколов беспроводной передачи данных IEEE 802.11x (802.11a, 802.11b и т.д.) [2]. Беспроводной сеть называется поскольку принимает и передает информацию с помощью радиоволн (происходит это за счет преобразования необходимой информации в радиоволны, а передача данных происходит с помощью встроенной антенны).

Несколько сетей могут существовать одновременно из-за того, что радиоволны передаются на разных частотах, которые еще называются каналами. Чтобы передать информацию устройству Wi-Fi, необходимо наложить данные на радиоволну. Процесс наложения данных на радиоволну называется модуляцией. 802.11x - является стандартом беспроводной сети, данный стандарт занимает два нижних уровня модели OSI (Open System Interconnection) [3] – физический и канальный. Именно эти уровни в большей мере отражают специфику локальных сетей. Следует понимать, как именно различается беспроводная сеть от кабельной на физическом и канальном уровне.

Беспроводная сеть отличается от кабельной на физическом уровне, поскольку физический уровень IEEE 802.11x – радиоканал. Данный уровень диктует параметры физической среды передачи данных и обеспечивает передачу сигнала двумя методами: методом прямой последовательности и методом частотных скачков. Канальный уровень обеспечивает управление доступом и разделятся на два подуровня: MAC - управление доступом к среде передачи данных и LCC - управление логическим каналом.

На канальном уровне отличие беспроводной сети в том, что на подуровне MAC используется полудуплексный режим передачи данных, а в кабельных сетях с архитектурой Ethernet - дуплексный режим. При увеличении частоты количество данных, которые можно передать по беспроводной сети, увеличивается, однако снижается радиус действия.

Wi-Fi сети не отличаются своей дальностью передачи данных. Наиболее распространенные стандарты Wi-Fi это стандарт 802.11a [4] , 802.11g [5] и 802.11ac [6]. Стандарт 802.11a славится высокой производительностью и скоростью. Особенность данного стандарта заключается в том, что из-за использования 5 ГГц частоты и модуляции OFDM у него увеличена скорость передачи данных и он поддерживает большую доступную частоту пропускания, которая, в свою очередь, позволяет иметь большее число одновременных беспроводных соединений. Стандарт 802.11g представляет собой высокоскоростной диапазон 2.4 ГГц. Особенность данного стандарта проявляется в высокой скорости передачи данных. Данный стандарт соединил в себе все лучшее от стандартов 802.11a и 802.11b. Стандарт 802.11ac – относительно новый, работает на частоте 5-6 ГГц и обеспечивает значительно большие скорости, как на точку доступа, так и на клиента. Беспроводные сети работают на частотах 2.4 ГГц либо 5 ГГц. Wi-Fi сети достаточно сильно подвержены риску несанкционированного доступа, следовательно на их защиту следует обратить особое внимание.

Механизмы защиты данных

Любые механизмы проектируют люди, а люди имеют свойство ошибаться, в связи с чем возникают ошибки, которые позволяют обойти любую защиту. Существует следующие способы защиты беспроводных сетей: протокол шифрования WEP [7], протокол шифрования WPA [8], протокол WPA2, стандарт

безопасности 802.1X, стандарт WPS, фильтрация по MAC адресу, скрытие SSID [9], запрет доступа к настройкам точки доступа или роутера через беспроводную сеть. Самый нераспространенный способ защиты, который на удивление все еще иногда используется, это отсутствие всякой защиты. Это означает, что точка доступа, как и клиент, вовсе не маскируют передачу данных. Так как почти любой беспроводной адаптер имеет возможность "прослушки" (вместо приема пакетов предназначенных только себе, будут приниматься все возможные пакеты), данный способ защиты вообще неактуален. К сожалению, такой принцип работы имеют проводные сети – при подключении к хабу или свичу (свич предварительно переведен в режим работы хаба) сетевой адаптер может получать пакеты от всех устройств в данном участке сети. Ввиду того, что к беспроводной сети можно подключиться из любого места (в радиусе действия сети), то завладеть вашими данными не составит труда. Но стоит отметить, если необходимо работать в такой сети, то необходимо использовать VPN и SSL. Проведенный опрос среди владельцев своих беспроводных сетей показал, что большинство стремится использовать надежную и проверенную защиту, однако не мал процент тех людей, которые пренебрегают проверенными способами защиты, и даже не подозревают, какая опасность грозит их личным данным. На удивление были люди, которые и вовсе не использовали в своих сетях никакую защиту, аргументируя это тем, что им нечего скрывать. Опрошенные компании утверждают, что они используют фильтрацию по MAC-адресу. На основе данного опроса был составлен рейтинг использования протоколов защиты Wi-Fi, который представлен на рис. 1.

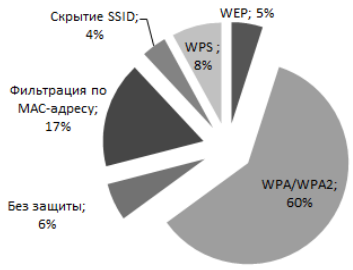


Рисунок 1 - Рейтинг использования протоколов защиты Wi-Fi

Следующим способом защиты является протокол шифрования WEP. WEP основан на алгоритме шифрования RC4 с 40 или 104 – битовым ключом, который складывается со сгенерированным вектором инициализации (24 бит). Благодаря полученному ключу по алгоритму RC4 шифруются данные пользователя и контрольная сумма. Вектор инициализации передается в открытом виде. Минусом данного алгоритма безусловно является 40-битный ключ. Следующим минусом является неизменяемость ключа, что существенно упрощает взлом. К сожалению, этот метод имеет серьезные недостатки, которые позволяют раскрыть передаваемую информацию, и предполагает распределение ключей шифрования вручную. Данным методом стоит пренебрегать наравне с открытыми сетями, поскольку он обеспечивает безопасность только на малый промежуток времени, спустя который передачу данных можно раскрыть. Главной уязвимостью WEP является ошибка в проектировании. Шифрование потока происходит благодаря временному ключу. WEP передаёт несколько байт данного ключа вместе с каждым пакетом данных. Это свидетельствует о том, что не смотря на сложность ключа, возможно раскрыть любую передачу, перехватив определенное количество пакетов. Шифрование WPA – замена уязвимому WEP. Расшифровывается, как Wi-Fi Protected Access.WPA призвана заменить WEP, и базируется на временном протоколе целостности ключей (TKIP), задача которого — не допустить повторного использования кодирующих ключей. WPA обеспечивает обратную совместимость с WEP, что позволяет использовать ее на той же аппаратной базе, а также гарантирует улучшенную защиту, взяв от WEP только все самое лучшее. С длиной пароля здесь лучше, чем в WEP, поскольку она случайная, и колеблется от 8 до 63 байт, благодаря чему его подбор становится в разы сложнее. Данный стереотип поддерживает некоторые алгоритмы шифрования передаваемых данных после рукопожатия: TKIP и CCMP. TKIP — среднее звено между WEP и WPA, был разработан для временной службы, пока в разработке находился CCMP. Следовательно, TKIP имеет некоторые уязвимости и является небезопасным. В данный момент времени используется исключительно в редком случае, иными словами, использование WPA с TKIP равняется использованию WEP. Особенностью TKIP является возможность проведения так называемой Michael-атаки. Разработчики предусмотрели недостатки своей технологии и в WEP в TKIP ввели некое ограничение, которое заключается в том, что если была обнаружена атака на подбор ключа, то точка доступа «засыпает» на 60 секунд. Суть Michael-атаки заключается в передаче «испорченных» пакетов для отключения сети. Отличие от DDoS-атаки заключается в том, что в данном случает хватит всего пары пакетов чтобы вывести точку доступа из строя на одну минуту. Отличие WPA от WEP заключается в том, что WPA шифрует данные каждого клиента по отдельности. Если рукопожатие было успешным, то после него будет сгенерирован временный ключ — PTK, который используется для кодирования передачи исключительно данного пользователя.

Следовательно, если злоумышленник проник в сеть, то прочитать пакеты других пользователей он сможет только после перехвата рукопожатия каждого из них. Несмотря на различные алгоритмы шифрования, WPA(2) также имеет два разных режима начальной аутентификации (проверки пароля для доступа клиента к сети) — PSK и Enterprise. PSK (еще называют WPA Personal) — вход по единому паролю, который вводит пользователь при подключении. На данный момент времени WPA/WPA2 уже является достаточно небезопасными, в связи с чем производители начинают выпускать новые обновления чтобы перекрыть старые уязвимости. Стандарт 802.1X позволяет производить аутентификацию и авторизацию устройств, пытающихся подключиться к локальной сети, и отказывает им в доступе, если аутентификация или авторизация не проходят. Администраторы беспроводных локальных сетей одними из первых внедрили стандарт 802.1X. В отличие от обычных проводных кабельных сетей беспроводные локальные сети нельзя «защитить» стенами и закрытыми дверями, поэтому они более уязвимы к нападениям. Сейчас стандарт 802.1X всё чаще применяется в кабельных сетях в качестве дополнительной меры защиты, и малоэффективен для беспроводных сетей.

WPS – стандарт полуавтоматического создания беспроводной сети. WPS позволяет клиенту подключиться к точке доступа по 8-символьному коду, состоящему из цифр (PIN). Благодаря ошибке в стандарте нужно подобрать только 4 символа. Следовательно, достаточно всего 10000 попыток подбора и, не смотря на сложность пароля, доступ будет получен. Беря во внимание то, что это взаимодействие происходит до всяких проверок безопасности, в секунду можно отправлять по 10-50 запросов на вход через WPS, и примерно через 5 часов доступ будет получен. Устройств, использующих данный тип защиты, сейчас примерно половина, следовательно, они очень уязвимы.

Атаки на беспроводные сети

Для проверки надежности беспроводной сети было разработано немало всевозможных методов [10]. Самой универсальной и распространенной атакой является взлом WPA/WPA2 паролей. Рейтинг способов атаки на беспроводные сети представлен на рис. 2.

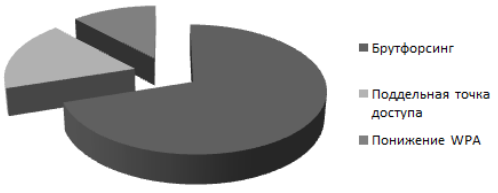


Рисунок 2 – Рейтинг способов атаки на Wi-Fi

Главным ее достоинством является то, что ее возможно применить к большинству сетей на данный момент времени. Одним из главных минусов является то, что для осуществлений данной атаки необходимо, чтобы к точке доступа был подключен клиент. Для успешного осуществления данной атаки необходимо знать название сети (ESSID), далее необходимо получить достаточно качественную запись процедуры обмена ключами между клиентом и точкой доступа (так называемый “хендшейк”, от англ. Handshake – рукопожатие), достаточно часто на данном этапе производится деаутентификация клиента, с целью заставить его заново подключится к сети, т.е. произвести рукопожатие. После захвата необходимых пакетов, необходимо произвести атаку «брутфорсингом» (методом перебора) паролей. Поскольку в перехваченном рукопожатии мы имеем хеш пароля, нам необходимо подбирать пароли до тех пор, пока у нас не будет точно такой же ответ, как и в перехваченном рукопожатии. Следовательно, если пароль будет достаточно надежным (под надежностью подразумевается длина пароля), то взломать такую сеть за короткий промежуток времени не удастся. Следующим типом атаки является атака на сети с использованием защиты WEP. Как упоминалось ранее, для его взлома необходимо просто перехватить необходимое количество пакетов, поскольку каждый пакет имеет несколько байт ключа. На данный момент времени точек, которые использовали бы WEP, почти нет, следовательно, данный способ теряет свою актуальность.

Далее рассмотрим обход стандарта полуавтоматического подключения WPS. Данный протокол описывался ранее, но стоит напомнить, что его обход не составит труда, поскольку он имеет всего 8 символов, и последний символ является контрольной суммой, следовательно стоит подобрать всего 7 символов. Первый блок состоит из 4 цифр, второй – из 3, это означает, что следует перебрать всего лишь 10998 комбинаций. На данный момент точек доступа со включенным WPS практически нет.

Теперь следует рассмотреть понижение протокола WPA до WEP. Данный способ касается социальной инженерии. Суть заключается в том, что каждый раз, когда клиент подключается к своей точке доступа, атакующий каждый раз отключает клиента от нее (производит деаутентификацию) при помощи отправки шифрованных пакетов данного протокола. Главной задачей является заставить клиента поверить в неработоспособность данного протокола (WPA) и заставить его перейти на другой протокол – WEP, либо отключить шифрование.

Следующим способом атаки является подмена настоящей точки доступа фальшивой. Идея заключается в том, что на точку доступа бесконечно отправляются пакеты деаутентификации, в

следствии чего клиент не может подключиться к точке. В это время человек, которому необходимо завладеть точкой, «поднимает» свою точку доступа, с такими же параметрами, как у необходимой сети и ожидает подключения клиента к ней. Следующим этапом является выманивание у клиента пароля сети, производится это совершенно разными способами, например: в браузере у пользователя будет окно очень схоже с окном подключения к точке доступа, где его попросят ввести пароль. Данный способ использует некомпетентность клиента.

Теперь рассмотрим атаку с помощью беспроводных сетей. Данный способ заключается в создании мошеннической точки доступа. Идея заключается в том, что злоумышленник создает свою точку, разумеется без пароля, и ждет пока к ней подключается клиенты. После подключения клиента к точке, злоумышленник может реализовать любую атаку для получения пароля клиента, куки клиента или перенаправить на различные сайты.

Выводы

Развитие беспроводных сетей несет в себе также и угрозы при работе в этих сетях. Таким образом, следует не пренебрегать безопасностью своей беспроводной сети и быть всегда внимательными, использовать только длинные пароли, через некоторый промежуток времени пароли следует менять. Рекомендуется для защиты своей сети использовать протокол WPA2-PSK-CCMP. Данный материал предоставлен исключительно в ознакомительных целях.

Литература

1. Wi-Fi // Wikipedia. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/Wi-Fi
2. Группа стандартов WiFi IEEE 802.11 // wi-life. [Электронный ресурс]. – Режим доступа: http://wi-life.ru/texnologii/wi-fi/wi-fi-standarty
3. Семиуровневая модель OSI // Sernam. [Электронный ресурс]. – Режим доступа: http://sernam.ru/book_icn.php?id=6
4. IEEE 802.11a // Wikipedia. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/IEEE_802.11a
5. IEEE 802.11g // Wikipedia. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/IEEE_802.11g
6. IEEE 802.11ac // Wikipedia. [Электронный ресурс]. – Режим доступа: https://ru.wikipedia.org/wiki/IEEE_802.11ac
7. Wi-Fi сети: проникновение и защита. 1) Матчасть. // Хабрахабр. [Электронный ресурс]. – Режим доступа: https://habrahabr.ru/post/224955/
8. Взлом Wi-Fi WPA/WPA2 для чайников // Variable. [Электронный ресурс]. – Режим доступа: http://variable.pp.ua/взлом-wi-fi-wpawpa2-для-чайников/
9. Что такое SSID беспроводной сети? // Netgear. [Электронный ресурс]. – Режим доступа: https://kb.netgear.com/ru/22374/Что-такое-SSIID-беспроводной-сети-1479991184049
10. Виды атак на Wi-Fi // Hackware. [Электронный ресурс]. – Режим доступа: https://hackware.ru/?p=158

Вязмин В. И., Чернышова А. В. Беспроводная технология Wi-Fi. Уязвимости и методы защиты. *В статье рассмотрены стандарты Wi-Fi, методы защиты и взлома беспроводных вычислительных сетей. Определены слабые стороны и подчеркнуты сильные стороны передачи данных с помощью технологии Wi-Fi.*

Ключевые слова: *Беспроводная вычислительная сеть, защита, атака, уязвимость, стандарт, данные.*

Vyazmin V. Chernyshova A. Wireless technology Wi-Fi. Vulnerabilities and methods of protection. The article considers Wi-Fi standards, methods of protection and hacking of wireless computer networks. *Weaknesses have been identified and the strengths of data transfer using Wi-Fi technology have been emphasized.*

Keywords*: Wi-Fi, protection, attack, vulnerability, standard, data.*

Статья поступила в редакцию 25 апреля 2018 г.
Рекомендована к публикации доцентом Зори С. А.

УДК 004.4

Исследование организации кроссплатформенной рабочей среды с облачным хранилищем данных

А. А. Когутенко, С. В. Плотникова
Государственное бюджетное нетиповое общеобразовательное учреждение
«Республиканский лицей-интернат «Эрудит» – центр для одаренных детей»
Министерства образования и науки Донецкой Народной Республики
and.kogutenko@yandex.ru

Когутенко А. А., Плотникова С. В. Разработка кроссплатформенной рабочей среды с облачным хранилищем данных. *В данной статье рассмотрены этапы создания кроссплатформенной рабочей среды с облачным хранилищем данных. Изучены особенности организации облачных хранилищ данных. Обоснован выбор операционной системы для сервера, проанализированы доступные способы обработки информации в веб-браузере (JavaScript и Flash). Рассмотрено применение и предназначение, достоинства и недостатки основных веб-серверов (Apache HTTP Server, Internet Information Services (IIS) и nginx), серверных языков (Hypertext Preprocessor (PHP), Python, Java, Ruby on Rails), серверных систем управления базами данных (MySQL, SQLite, PostgreSQL) с целью выбора оптимальных инструментов для разработки и обеспечения работоспособности среды. Описана организация системы, определены ключевые моменты политики безопасности (безопасность рабочей среды, безопасность хранилища данных), основной функционал системы.*

Ключевые слова: *WebOS, облачное хранение данных, веб-браузер, расширяемое веб-приложение, JavaScript, Debian, Apache, nginx, MySQL. PHP.*

Введение

В современном мире существует множество различных технологий, одной из которых является облачное хранение данных, дающее доступ к ним из любой точки Интернета и уверенность в сохранности файлов. Есть сервисы, позволяющие хранить информацию удобно и надёжно (Яндекс.Диск [1], Dropbox [2] и т. п.). Однако подобные сервисы не позволяют работать с данными непосредственно из веб-браузера, или же предоставляют крайне ограниченный функционал. Появляется необходимость в разработке расширяемого веб-приложения, которое позволило бы работать с данными и облаком, а именно виртуальный рабочий стол в браузере.

Актуальность разрабатываемой системы заключается в доступе к рабочей среде и облаку непосредственно в веб-браузере – на любом компьютере, ноутбуке, планшете с установленным браузером и доступом к сети Интернет или локальной сети.

Цель статьи: исследовать организацию расширяемой кроссплатформенной рабочей среды с облачным хранилищем данных.

В соответствии с целью в статье ставятся и решаются следующие задачи:

- изучить способы обработки данных посредством веб-браузера.
- исследовать методы организации серверной части приложения.
- спроектировать архитектуру системы: технологии поддержки приложений, процесс обмена данными с облаком.

При использовании виртуального рабочего стола в браузере пользователь имеет следующие преимущества:

- легко переходить с устройства на устройство, работая при этом с актуальными данными из облака;
- в случае поломки устройства данные останутся в облаке, таким образом устраняются проблемы потери данных из-за возможной неисправности накопителей;
- защищённость данных обеспечивается шифрованием на стороне клиента.

Особенности организации облачных хранилищ данных

Облачное хранилище – онлайн-хранилище, в котором данные хранятся на множестве распределённых в сети серверов. То есть, пользователям выделяется пространство на серверах и они получают к нему доступ.

Обычно облачные хранилища работают следующим образом. Как только пользователь начинает загрузку файла в облако, промежуточный сервер делает запрос серверам хранилища на выделение свободного места. С

получением ответа, в котором указывается внутренний адрес сервера с выделенным пространством (что должно происходить почти мгновенно), соединяется с сервером хранилища и передаёт данные непосредственно ему. На серверах хранилища при получении файла сразу же происходит резервное копирование.

Также немаловажную роль играет операционная система, используемая на серверах. От неё требуется надёжность, стабильность работы, производительность и безопасность. Кроме того, изучению и сравнению подлежат принципы работы файловых систем.

Способы обработки данных посредством веб-браузера

Проанализируем доступные способы обработки информации в веб-браузере, их достоинства и недостатки.

Существует две основные технологии, поддерживаемые современными браузерами – JavaScript и Flash [3]. JavaScript поддерживается наверняка, так как встроен непосредственно в веб-обозреватель и поставляется со всеми современными браузерами. Flash является также довольно популярной технологией, но для его установки необходимо скачивать отдельную программу. В настоящее время JavaScript является лучшим выбором для создания интерактивных веб-страниц. Однако во время реализации поддержки работы с микрофоном и камерой не стоит забывать о Flash, так как мультимедийные функции не в полной мере поддерживаются JavaScript. Идеальным вариантом будет комбинирование JavaScript и Flash.

Организация серверной части приложения

Среда обработки *информации.*

Важной составляющей организации работы сервера является выбранная операционная система её надёжность, безопасность и гибкость.

Windows Server хоть и стабильна, но содержит большое количество уязвимостей и является коммерческим продуктом.

Из дистрибутивов Linux одним из самых стабильных является Debian [4]. Операционные системы на базе Linux и BSD очень гибки и имеют бесплатную лицензию. Однако размер ядра Linux постоянно увеличивается; увеличивается и количество уязвимостей в нём.

Известно, что операционные системы семейства BSD отличаются высокой надёжностью и стабильностью. Помимо того, они безопасны и производительны. Вероятность нахождения ошибки в BSD ниже, чем в Linux и Windows Server [5].

Так или иначе, выбор падает на Debian или FreeBSD.

Веб-сервер.

Лидирующие места занимают Apache HTTP Server, Internet Information Services (IIS) и nginx. Возможно разработать новый веб-сервер конкретно для поставленной задачи, однако этот вариант не является надёжным и безопасным. Поэтому лучше использовать решения, зарекомендовавшие себя и проверенные временем.

Рассмотрим применение и предназначение каждого из выбранных серверов.

Веб-сервер Apache [6] создавался для обработки запросов и отдачи контента. К его достоинствам можно отнести гибкость, надёжность, кроссплатформенность, поддержку модулей. Недостатком является его средняя производительность.

Веб-сервер nginx [6] предназначен для отдачи статических данных и передачи динамических запросов другому программному обеспечению для обработки, может использоваться, как прокси. Достоинствами nginx является эффективное потребление ресурсов, кроссплатформенность, возможно использовать, как прокси. Также данный сервер превосходен для отдачи статического контента. Среди недостатков можно отметить среднюю гибкость.

Веб-сервер IIS [7] используется для размещения сайтов в сети Интернет. Его достоинствами являются безопасность, удобство администрирования, а недостатками – средняя производительность, совместимость только с Windows.

Все три веб-сервера поддерживают безопасность на должном уровне. Apache хорошо подходит для обработки информации, nginx – для отдачи статических данных. Также в nginx стоит отметить большую отказоустойчивость, чем в остальных. Так как требуется одновременно быстрое и мощное решение, то лучше всего использовать Apache и nginx в связке: nginx как front-end (для получения запросов и передачи на обработку другому ПО), а Apache – как back-end, для получения и обработки запросов от nginx.

Способ обработки *информации.*

Большое значение имеет выбор языка программирования, позволяющего писать программы/скрипты для обработки данных и генерации динамического контента.

Основными серверными языками являются Hypertext Preprocessor (PHP), Python, Java, Ruby on Rails.

Предпочтение отдаётся производительным и потребляющим мало памяти языкам. Для сравнения эффективности языков были взяты результаты тестирования.

Таблица 1. Сравнение языков программирования по времени работы программы

Операция\Язык	Время выполнения (секунды)			
	PHP	Python	Java	Ruby
Множество Мандельброта	125,17	273,43	7,1	~420
Норма матрицы	37,94	188,83	4,29	141,49
k-нуклеотид	43,96	84,73	7,93	101,95
Задача n тел	~300	~780	21,54	290,75
Сходство белков	59,37	110,91	2,13	77,16
Число π	2,15	–	3,06	3,14
Комплементарность	2,81	2,82	1,1	4,03
Двоичные деревья	88,07	86,9	11,26	54,24
Регулярные выражения	3,34	14,86	12,31	28,8

Таблица 2. Сравнение языков программирования по использованию памяти

Операция\ Язык	Использованная память (КБ)			
	PHP	Python	Java	Ruby
Множество Мандельброта	8,688	13,748	27,108	69,656
Норма матрицы	8,796	9,016	29,884	10,036
k-нуклеотид	235,632	221,028	185,16	133,912
Задача n тел	8,668	7,728	27,092	8,916
Сходство белков	8,812	8,024	28,824	9,712
Число π	9,856	–	31,76	163,316
Комплементарность	359,768	265,428	294,36	133,304
Двоичные деревья	734,364	274,404	520,676	434,456
Регулярные выражения	158,792	439,208	834,824	260,46

Относительно неплохие результаты показывает Java, однако при выполнения некоторых заданий иногда имеет неоправданный расход памяти. Python и Ruby временами выполняются дольше, чем PHP. Для разработки серверной части приложения целесообразно выбрать PHP.

Необходимо определиться с системами управления базами данных, поскольку база данных – хранилище на сервере для различных типов данных, которое достаточно сильно влияет на производительность и стабильность системы.

Так как от базы данных, в первую очередь, требуется надёжность и высокая скорость работы, есть смысл говорить о разработке таковой на производительном языке программирования. Это позволило бы разработчикам полностью осознать принцип работы СУБД и, как следствие, сделать её гарантированно качественной и надёжной.

Рассмотрим три основные серверные СУБД: MySQL, SQLite, PostgreSQL [8].

Таблица 3. Сравнение серверных СУБД

Достоинства	Недостатки
MySQL	
Простота в работе. Богатый функционал. Безопасность. Масштабируемость. Скорость.	Есть ограничения. Проблемы с надёжностью. Медленно развивается.
SQLite	
Состоит из одного файла. Использует язык SQL. Подходит для разработки и тестирования.	Отсутствие системы пользователей. Отсутствие возможностей увеличения производительности. Разрешён только один процесс записи в промежуток времени.
PostgreSQL	
Большое количество дополнений. Объектность.	Низкая производительность.

MySQL, имея довольно высокую скорость и безопасность в работе, также обладает большим количеством функций обработки данных.

Исходя из анализа способов организации серверной части, в качестве операционной системы будет выступать FreeBSD. Уверенно можно сказать, что в идеале необходимо использовать Apache и nginx в связке: nginx для отдачи статического контента и передачи внешних запросов внутреннему ПО (Apache с дополнениями). Надёжное хранилище структурированной информации обеспечит MySQL.

Проектирование системы. Построение базовых концепций

Весь функционал реализован в виде веб-сайта. Сначала посетитель попадает на страницу приветствия, описывающую сервис. Там же расположены ссылки на страницы входа и регистрации.

После входа или регистрации пользователь видит персональный рабочий стол (также в виде

веб-страницы). Некоторые базовые программы, такие как «Настройки» и «Магазин приложений» уже установлены. На использование приложений накладываются некоторые ограничения.

Безопасность *рабочей среды.*

В целях создания безопасной рабочей среды, любое изменение в облаке должно производиться только с помощью функции API. Целесообразно создать отдельный интерпретатор программного кода, так как использование JavaScript для написания пользовательских программ и его встраивание непосредственно в код страницы не обеспечивает безопасность рабочей среды.

Безопасность *хранилища.*

Основные требования к алгоритму шифрования на стороне клиента – производительность и надёжность. Как показывает практика и тесты, наиболее подходящим является алгоритм AES-256. Он существует уже достаточно долго (создан в 1998 году [9]) и успел зарекомендовать себя в качестве быстрого и надёжного алгоритма.

Помимо обычного шифрования может возникнуть потребность в необратимом шифровании (хешировании). Для таких целей целесообразно использовать SHA-512, однако он имеет слишком большую длину и его лучше использовать исключительно для обеспечения безопасности. В случае проверки целостности файлов с помощью контрольных сумм можно применить CRC-32, так как этот алгоритм выдаёт достаточно короткий результат. Проверка целостности информации может пригодиться при запросе пользователем файлов из облака.

Ограничения *на использование приложений.*

По уровню привилегий приложения можно разделить на два класса – системные и пользовательские. Системные приложения не подлежат удалению и имеют повышенные привилегии. Скорее всего, они будут реализованы на «чистом» JavaScript.

Функционал *системы.*

В первую очередь, система должна предоставлять платформу для запуска программ. В её функции входит:

- интерпретация пользовательских программ
- предоставление функций API для приложений
- шифрование передаваемых данных

Помимо того, система должна взаимодействовать с пользователем (с помощью графической оболочки) и иметь в своём составе компоненты для настройки оболочки. Они представляют собой системные приложения.

Выводы

Основной целью является исследование процесса разработки расширяемого приложения для работы с облачным хранилищем. Под расширяемостью предполагается предоставление возможности написания пользовательской программы с использованием API (программный интерфейс приложения), предоставляемого сервисом. Рабочей средой приложения будет являться современный веб-браузер (Chrome, Opera, Firefox).

В процессе рассмотрения структуры облачных систем и технологий обработки информации были рассмотрены такие основные моменты, как:

- устройство облачных систем.
- технологии обработки информации средствами веб-браузера.
- организация серверной части приложения (хранилища): выбор программного обеспечения, наилучшей их компоновки.

Выбрана наиболее подходящая конфигурация для серверных задач. Так, в качестве операционной системы выбрана FreeBSD, так как имеет высокую стабильность и надёжность. Веб-сервером будет комбинация apache и nginx. Базой данных будет выступать MySQL, благодаря хорошей скорости работы и функциональности. В качестве языка программирования для разработки серверной части выбран PHP.

Литература

1. Яндекс.Диск [Электронный ресурс] – 2017 – Режим доступа: https://disk.yandex.ua/ – Загл. с экрана.

2. Dropbox [Электронный ресурс] – Режим доступа: https://www.dropbox.com/ru/

3. Кантор И. Современный учебник Javascript. [Электронный ресурс] – 2017 – Режим доступа: https://learn.javascript.ru/intro – Загл. с экрана.

4. Причины выбрать Debian [Электронный ресурс] – 2017 – Режим доступа: https://www.debian.org/intro/why_debian.ru.html – Загл. с экрана.

5. Почти объективно на тему «чем FreeBSD лучше Linux» [Электронный ресурс] – 2017 – Режим доступа: http://eax.me/freebsd-vs-linux/ – Загл. с экрана.

6. Apache vs Nginx: практический взгляд [Электронный ресурс] – 2017 – Режим доступа: https://habrahabr.ru/post/267721/ – Загл. с экрана.

7. Apache или IIS – сравнение и преимущества [Электронный ресурс] – 2017 – Режим доступа: http://wiki.merionet.ru/servernye-resheniya/3/apache-ili-iis/ – Загл. с экрана.

8. SQLite vs MySQL vs PostgreSQL: сравнение систем управления базами данных [Электронный ресурс] – 2017 – Режим доступа: http://devacademy.ru/posts/sqlite-vs-mysql-vs-postgresql/ – Загл. с экрана.

9. Advanced Encryption Standard [Электронный ресурс] – 2017 – Режим доступа: https://ru.wikipedia.org/wiki/Advanced_Encryption_Standard – Загл. с экрана.

Когутенко А. А., Плотникова С. В. Разработка кроссплатформенной рабочей среды с облачным хранилищем данных. *В данной статье рассмотрены этапы создания кроссплатформенной рабочей среды с облачным хранилищем данных. Изучены особенности организации облачных хранилищ данных. Обоснован выбор операционной системы для сервера, проанализированы доступные способы обработки информации в веб-браузере (JavaScript и Flash). Рассмотрено применение и предназначение, достоинства и недостатки основных веб-серверов (Apache HTTP Server, Internet Information Services (IIS) и nginx), серверных языков (Hypertext Preprocessor (PHP), Python, Java, Ruby on Rails), серверных систем управления базами данных (MySQL, SQLite, PostgreSQL) с целью выбора оптимальных инструментов для разработки и обеспечения работоспособности среды. Описана организация системы, определены ключевые моменты политики безопасности (безопасность рабочей среды, безопасность хранилища данных), основной функционал системы.*

Ключевые слова: *WebOS, облачное хранение данных, веб-браузер, расширяемое веб-приложение, JavaScript, Debian, Apache, nginx, MySQL. PHP.*

Kogutenko A. A., Plotnikova S. V. Development of cross-platform working environment with the cloudy depository of information. *The stages of creation of cross-platform working environment with the cloudy depository of information are considered in this article. The features of organization of cloudy depositories of information are studied. The choice of the operating system for a server is grounded, the accessible methods of treatment of information in a web-browser are analysed (JavaScript and Flash). Application and destiny, dignities and lacks of basic web-servers (Apache HTTP Server, Internet Information Services (IIS) and nginx), server languages (Hypertext Preprocessor (PHP), Python, Java, Ruby on Rails), server control systems by databases with the purpose of choice of optimum instruments for development and providing of capacity of environment is considered. Organization of the system is described, the key moments of policy of safety (safety of working environment, safety of depository of information), basic functional of the system, are certain.*

Keywords: *WebOS, cloudy data storage, web-browser, extended web-appendix, JavaScript, Debian, Apache, nginx, MySQL. PHP.*

Статья поступила в редакцию 25 апреля 2018 г.
Рекомендована к публикации доцентом Зори С. А.

УДК 343.2/.7

Киберпреступность в России. Юридическая ответственность за нарушения прав в сфере информационных технологий

А. Н. Прикмета
Липецкий государственный технический университет, г. Липецк
parapan58@gmail.com

Прикмета А. Н. Киберпреступность в России. Юридическая ответственность за нарушения прав в сфере информационных технологий. *Статья посвящена рассмотрению вопросов* ***к****иберпреступности в России. Дается анализ понятий «киберпреступность», «киберкриминальный рынок», оцениваются причины и особенности киберпреступлений. Особое внимание уделяется юридической ответственности за нарушения прав в сфере информационных технологий.*

Ключевые слова: *киберпреступность, киберкриминальный рынок, киберинциденты, ответственность за киберпреступления.*

Введение

В наше время не осталось сфер, где в той или иной мере не применялись бы информационные технологии и программное обеспечение. С развитием современных технологий сформировались условия появления нового вида преступлений, совершаемых в киберпространстве. Современный мир – сфера компьютерных технологий, в котором кибервойны и киберпреступления стали реальностью.

По определению экспертов ООН термин «киберпреступность» охватывает любое преступление, которое может совершаться с помощью компьютерной системы или сети, в рамках компьютерной системы или сети или против компьютерной системы или сети. Таким образом, к киберпреступлениям может быть отнесено любое преступление, совершенное в электронной среде [1].

По исследованиям The Wall Street Journal:

- ✓ 29 стран имеют специализированные военные киберподразделения, занимающиеся противодействием угрозам информационной безопасности, в частности Россия, Австралия, Бразилия и Египет;
- ✓ 49 стран закупают специализированное хакерское программное обеспечение, в том числе Россия, Австралия, Бразилия и Египет;
- ✓ 63 страны используют инструменты сплошного наблюдения как внутри страны, так и глобально (Чехия, Италия, Мексика и др.).

Согласно информации о взломах, наиболее развитым кибероружием обладают Россия, США, Великобритания, Китай, Индия, Иран и Северная Корея.

Отчет консалтинговой компании PricewaterhouseCoopers (PwC) показывает, что стратегию по кибербезопасности имеют 60% российских и американских компаний. В Германии только 45%, во Франции 51%, в Италии 55%. Наиболее защищенными от кибератак странами являются Малайзия (74%), Япония (72%) и Индонезия (70%)[2].

Для создание и использование кибервооружений не требует колоссальных вложений в обогатительные заводы, разработку средств доставки и строительство пусковых установок. Достаточно обладать сравнительно небольшими финансовыми ресурсами, средними компьютерными системами и доступом к глобальным сетям. Кибератаки сложно остановить и зачастую невозможно отследить. Благодаря этому инструменты хакерских атак стали доступны не только правительствам, но и агрессивным политическим группировкам и террористическим организациям.

На расширенном заседании Совета безопасности 26.10.2017, президент России В.В.Путин обозначил основные направления развития информационной безопасности в Российской Федерации, среди которых выделил увеличение интенсивности кибератак. По его словам, все острее встает проблема вторжения в ИТ-системы в сфере гособороны и управления, а также финансов. Кроме того, значительную угрозу представляет утечка электронных документов.

«*Следует повысить безопасность и устойчивость работы инфраструктуры российского сегмента Интернета. Как и в других демократических странах, мы должны бороться с теми, кто использует информационное пространство для пропаганды радикальных идей, оправдания терроризма, экстремизма, решительно пресекать попытки размещения материалов, угрожающих безопасности нашего государства, общества в целом и отдельных граждан...*» [3].

Исследования

Классификация киберпреступлений. Поскольку киберпреступления охватывают широчайший пласт общественных отношений, предполагают использование различного оборудования и имеют целый спектр способов совершения, логично провести их классификацию.

Согласно классификации установленной Конвенцией Совета Европы виды киберпреступлений объединены в пять групп:

1. Компьютерные преступления, направленные против компьютерных данных и систем (например, взлом базы данных мобильного оператора с целью получения паспортных данных пользователей). Классифицируются как *незаконный доступ.*

2. Противоправные деяния, связанные с использованием технологий (подлог, извлечение, блокировка или изменение данных, мошенничество, получение экономической выгоды иными способами), так называемый *незаконный перехват*.

3. Противоправные деяния, связанные с содержанием данных или контентом. Самый распространённый и жёстко наказуемый практически во всех странах вид этих киберпреступлений – преступные деяния, связанные с детской порнографией.

4. Нарушение авторских и смежных прав, определяемое как *вмешательство в данные.* При этом установление таких правонарушений Конвенцией отнесено к компетенции национальных законодательств государств.

5. Кибертерроризм и использование виртуального пространства для совершения актов насилия, а также другие деяния, посягающие на общественную безопасность. Так называют *особо серьезные преступления*, связанные с жестокостью и совершением актов насилия по средствам высоких технологий. Также к этому виду относят деяния, которые ставят под угрозу общественную безопасность, а также акты расизма и ксенофобии, совершённые с использованием компьютерных сетей[4].

При этом в Конвенции вредоносное программное обеспечение понимается как средство, способствующее совершению компьютерных преступлений, а его использование не является отдельным правонарушением.

Количество киберпреступлений неуклонно растет. По данным испанского сайта Informática Forense (Компьютерная криминалистика) [5] только на 2017г. прогнозируется более 26500 кибератак против государственного сектора и стратегических компаний, что на 26.5% больше, чем в 2016г. (см. рис.1).

Рисунок 1 – Тенденции изменения числа кибератак

Более 70 кибератак было зафиксировано в октябре 2017г., что связывают с проведением референдума в Каталонии. Их целью были сайты правительственных организаций, Конституционный суд, Национальный разведывательный центр и др.

Как видим, кроме экономической составляющей, в данный момент причиной киберпреступлений может быть и составляющая политическая[6].

Исследования «Лаборатории Касперского» показали, что за год каждая вторая промышленная компания в мире пережила от одного до пяти киберинцидентов, которые затронули важные инфраструктуры или автоматизированные системы управления технологическими процессами, см. рис 2.

Опрос, проводимый более, чем в 350 организациях по всему миру, показал, что три четверти компаний допускают вероятность пострадать от кибератак [7].

Особенностями данного вида преступлений являются:

- чрезвычайная скрытность деяний, которая достигается применением механизмов анонимности и шифрования;
- трансграничность: преступник и жертва могут быть разделены тысячами километров, границами нескольких государств;
- нестандартность способов совершения;
- автоматизированный режим.

Самым разрушительным образцом американского кибероружия стал червь Stuxnet, который вывел из строя центрифуги на иранском заводе по обогащению урана.

Успешность применения кибероружия можно проиллюстрировать на примере конфликта в Сирии. По данным компании в области

компьютерной безопасности FireEye, сирийское правительство совершило атаку на компьютерные системы командования повстанцев и получило важную тактическую информацию, что вылилось в значительные потери для повстанцев.

Рисунок 2 – Причины киберинцидентов

Киберкриминальный рынок. Киберкриминальный рынок рассматривается как совокупность «услуг» и «продуктов», используемых для совершения противоправных действий в киберпространстве.

Продукты:

✓ программное обеспечение, предназначенное для получения несанкционированного доступа к компьютеру или мобильному устройству, кражи данных с зараженного устройства и/или денежных средств со счета жертвы (троянцы);

✓ программное обеспечение, предназначенное для эксплуатации уязвимостей в установленном на компьютере ПО (эксплойты).

Услуги:

✓ рассылка спама;

✓ организация DDoS-атак (перегруз сайтов запросами с целью сделать их недоступными для легитимных пользователей);

✓ «перекриптовка» вредоносного ПО (изменение вредоносного ПО таким образом, чтобы его не детектировали антивирусы);

✓ VPN (предоставление анонимного доступа к веб-ресурсам);

✓ передача в аренду ботнетов;

✓ проверка ценности краденных данных платежных карт;

✓ услуги по подтверждению данных (фальшивые звонки, фальшивые сканы документов);

✓ продвижение вредоносных и рекламных сайтов в поисковой выдаче;

✓ посредничество при сделках по приобретению «продуктов» и «услуг»;

✓ вывод и обналичивание средств.

По наблюдениям экспертов «Лаборатории Касперского», преступления, связанные с кражей денег, наиболее распространены в последние годы.

По данным аналитического центра Zecurion веб-сервисы являются самым популярным в мире каналом утечек информации (26,7%), на втором месте – неэлектронные носители. В России 53% компаний сталкиваются с утечкой информации через электронную почту, 32% - через интернет-сервисы, см. рис.3 [8].

Рисунок 3 –Каналы утечек информации

Ответственность за киберпреступления в законодательстве РФ.

Актуальность темы киберпреступлений придает тот факт, что размер причиняемого этим видом преступлений, ущерба неуклонно растет и по мнению ряда экспертов доходы теневого бизнеса сети Интернет могут сравниться с прибылью от незаконной торговли наркотиками.

В Росси совершается в среднем ежедневно 44 хищения из систем дистанционно – банковского обслуживания.

Согласно статистическим данным Европола большинство хакеров и киберпреступников – граждане России и СНГ.

В настоящее время не существует ни релевантной статистики, отражающей реальную картину состояния рынка киберпреступлений, ни методов сбора данных такого вида.

Поэтому столь важна разработка методов анализа, сбора информации, а также уровень ее классификации.

Киберпреступность представляет собой не только техническую и правовую, но и социальную проблему, эффективное решение которой требует системного подхода.

По данным Global CIO доля привлеченных к ответственности за киберпреступления менее 0,1% .

Основная проблема – отсутствие реальной ответственности киберпреступников за преступления.

Лишь 3% из поданных заявлений доходят до возбуждения уголовных дел. Следует учитывать, что данные по компьютерному преступлению собрать весьма сложно, электронные улики остаются, но их легко уничтожить и сложно обеспечить их юридическую значимость.

Ответственность за свои действия несут в среднем лишь 5-7 преступников.

Причин этому несколько.

1. Очень часто преступные группировки находятся в разных городах, нередко – в разных странах.

Последние несколько лет в связи с появлением и распространением ботнетов[1] ситуация усложнилась еще более. Деньги крадутся у компании, находящейся в одном регионе, через банк в другом, переводятся через несколько счетов в разных банках и платежных системах и обналичиваются в третьем.

Возникает вопрос, какой территориальный орган должен возбуждать дело? По действующему законодательству дело возбуждает тот орган, на территории которого произошло преступление. Другой пример. Сервер атаки находится в Германии, а цель – предприятие/банк в Москве. Эти вопросы, связанные с местоположением преступников и целью киберпреступлений, законодательно не решены, что служит основанием в отказе в возбуждении дела.

2. SMS-мошейничество вообще не попадает под действующие нормы, поскольку сумма конкретного ущерба очень мала и на этом основании органы могут отказать в возбуждении дела. Отметим, что, по мнению экспертов, оборот SMS-мошейничества оценивается в 100 млн. руб. в месяц.

3. Квалификация следователей. Вряд ли следует надеяться, что следователь территориального органа внутренних дел с минимальной компьютерной грамотностью, сможет расследовать преступление, охватывающее несколько регионов. Эта проблема заключается в недостаточной подготовленности сотрудников правоохранительных органов в области IT-систем, интернет-технологий, программного обеспечения.

Опросы среди следователей показывают, что 95% респондентов получили юридическое образование. И только 5% обладают еще и образованием по специальности «Информатика и вычислительная техника». 63% опрошенных владеют компьютером на уровне «среднего пользователя», 37% - на уровне «продвинутого пользователя». 79% при этом постигают компьютер самостоятельно, курсы для сотрудников правоохранительных органов посещали только 21%, и незначительный процент (5%) – коммерческие курсы.

Несмотря на это, следует отметить, что Россия была одной из первых держав, создавшая еще в 90-х годах киберполицию, а в 2014 были созданы кибервойска. По оценкам экспертов, Россия находится в первой пятерке государств мира по уровню развития кибервойск.

4. Учитывая, что в случае уголовного расследования убытки от расследования могут оказаться выше суммы причиненного ущерба, многие организации предпочитают ограничиваться разрешением конфликта своими силами.

5. Боязнь подрыва собственного авторитета в деловых кругах и как результат этого — потеря значительного числа клиентов. Эго обстоятельство особенно характерно для банков и крупных финансово-промышленных организаций, занимающихся широкой автоматизацией своих производственных процессов.

6. Боязнь возможности выявления в ходе расследования собственного незаконного механизма осуществления отдельных видов деятельности и проведения финансово-экономических операций.

7. Правовая и законодательная неграмотность пострадавших[9,10].

8. Судебная система фундаментально не готова рассматривать цифровые доказательства ни в арбитражном, ни уголовном процессе. Когда

[1] Слово Botnet (ботнет) образовано от слов «robot» (робот) и «network» (сеть). Киберпреступники используют специальные троянские программы, чтобы обойти систему защиты компьютеров, получить контроль над ними и объединить их в единую сеть (ботнет), которой можно управлять удаленно.

банк идет в суд с доказательствами в виде IP-адресов, его просят предоставить документ, заверенный подписью.

9. Несвоевременность выявления киберпреступлений. В соответствии с результатами опросов:

- ✓ в 53% случаев с момента совершения преступления до поступления информации о совершенном преступлении проходит более 10 дней;
- ✓ 73% респондентов отметили запоздалое начало предварительного расследования, когда многие важные доказательства уже утрачены.

В юридической науке до сих пор остается открытым вопрос об ответственности, которая должна применяться к правонарушителям в сфере компьютерной информации. Одни исследователи полагают, что так как компьютеризация общества распространяется во все сферы жизнедеятельности, то к правонарушителям должно применяться столько видов ответственности сколько существует в юридической науке, то есть: конституционная, уголовная, административная, дисциплинарная и гражданско-правовая, а в некоторых случаях и материальная.

Другие же придерживаются трех видов ответственности: 1) уголовной, 2) административной и 2) гражданской.

Наибольшую роль по юридической нагрузке играет уголовная ответственность. В Уголовном кодексе Российской Федерации часть преступлений выделены в отдельную главу 28 «Преступления в сфере компьютерной информации»:

- ✓ статья 272. Неправомерный доступ к компьютерной информации;
- ✓ статья 273. Создание, использование и распространение вредоносных компьютерных программ;
- ✓ статья 274. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей.

Статья 272 УК РФ. Неправомерный доступ к компьютерной информации.

По этой статье предусмотрено наказание, в виде «штрафа в размере до трехсот тысяч рублей, либо исправительными работами на срок до двух лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок.

В случае совершения группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет, либо ограничением свободы на срок до четырех лет, либо принудительными работами на срок до пяти лет, либо лишением свободы на тот же срок. Если же они повлекли тяжкие последствия или создали угрозу их наступления, – наказываются лишением свободы на срок до семи лет[11].

Объективной стороной состава данного преступления является неправомерный доступ к охраняемой законом компьютерной информации. Под таким доступом понимается получение возможности ознакомиться и/или воспользоваться ею. Сам доступ может выражаться в проникновении в компьютерную систему путем использования специальных технических или программных средств, которые позволяют преодолеть установленные системы защиты, а так же незаконное использование паролей или кодов, либо совершения иных действий в целях проникновения в сеть или систему под видом законного пользователя. Неправомерным признается доступ лица, не имеющего права на работу и получения данной информации, в отношении которых приняты специальные защитные меры, ограничивающие круг лиц имеющих к ним доступ.

Охраняемая законом информация – те данные, для которых установлен специальный режим правовой защиты, например государственная, служебная и коммерческая тайна, персональные данные, объекты авторского права и смежных прав.

Данный состав носит материальный характер и предполагает обязательное наступление одного или нескольких указанных в законе последствий: уничтожение, блокирование, модификация (переработка), копирование информации. Одним из важных моментов является установление причинной связи между несанкционированным доступом и наступлением последствий. Данное преступление считается оконченным в момент наступления последствий.

Субъективная сторона характеризуется умышленной формой вины.

Субъект преступления – любое вменяемое лицо достигшее 16 летнего возраста.

Пример: По приговору Орджоникидзевского районного суда г. Екатеринбурга 25.06.2017г., гр. Александровскому по совокупности преступлений назначено наказание в виде лишения свободы на срок 2 года за преступления предусмотренные ч. 3 ст. 183 Уголовного Кодекса Российской Федерации, то есть незаконное разглашение сведений, составляющих

коммерческую тайну без согласия их владельца лицом, которому она была доверена по работе, совершенное из корыстной заинтересованности и ч. 2 ст. 272 Уголовного Кодекса Российской Федерации, то есть как совершение неправомерного доступа к охраняемой законом компьютерной информации, повлекшее копирование компьютерной информации, совершенное из корыстной заинтересованности, совершенное группой лиц по предварительному сговору.

Статья 273 УК РФ. Создание, использование и распространение вредоносных компьютерных программ.

Наказание – принудительные работы на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей.

В случае совершения группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно причинившие крупный ущерб или совершенные из корыстной заинтересованности, - наказываются лишением свободы на срок до пяти лет со штрафом в размере от ста тысяч до двухсот тысяч рублей с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет или без такового.

Преступление считается оконченным с момента создания, изменения, использования или распространения вредоносной программы, создающей угрозу указанных в законе последствий.

Объектом преступления является общественная безопасность и общественный порядок, а также совокупность общественных отношений по правомерному и безопасному использованию информации.

Объективную сторону составляет сам факт создания компьютерных программ или иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Наиболее распространенными видами вредоносных программ являются компьютерные вирусы, черви, программы-сканеры, эмуляторы электронных средств защиты, программы управления потоками компьютерной информации, программы - патчеры.

Субъект – физическое, вменяемое лицо, достигшее 16 летнего возраста.

Субъективная сторона – вина в форме прямого умысла.

Данная статьей, имеет некоторые общие черты с составом преступления, предусмотренного ст. 272 УК. Сложность разграничения этих преступлений заключается в том, что неправомерный доступ к компьютерной информации (ст. 272 УК РФ), создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК РФ) ведут к несанкционированному уничтожению, блокированию, модификации либо копированию информации или нейтрализации средств защиты компьютерной информации.

Предметом преступления, предусмотренного ст. 272 УК, является только та информация, которая охраняется законом. Предметом же ст. 273 УК является создание, использование и распространение вредоносных программ, а так же любая информация, заведомо предназначенная для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации.

Состав преступления, предусмотренный частью 1 статьи 273 - формальный. Для признания преступления оконченным не требуется реального наступления вредных последствий

Пример: Приговор Лямбирского районного суда Республики Мордовия от 3.10.2017 г. в отношении Галабир С.В. о наказании на срок 1 год 6 месяцев ограничения свободы за преступления предусмотренные ч.1 ст. 273, ч. 2 ст. 273 и ч. 2 ст. 273. Гр. Галабир, использовал вредоносные компьютерные программы, заведомо предназначенные для несанкционированного копирования компьютерной информации из корыстной заинтересованности:

- совершил действия по созданию и распространению компьютерной программы, заведомо предназначенной для несанкционированной модификации и копирования компьютерной информации, совершенные из корыстной заинтересованности,
- совершил действия по использованию вредоносной компьютерной программы, заведомо предназначенной для нейтрализации средств защиты компьютерной информации и преступления.

Статья 274 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей. Наказывается штрафом в размере до пятисот тысяч рублей, либо исправительными работами до одного года, либо ограничением свободы на срок до двух лет, либо лишением свободы на тот же срок. В случае если такое деяние повлекло тяжкие последствия или создало угрозу их наступления, то наказывается принудительными работами на срок до пяти лет либо лишением

свободы на тот же срок.

Объективная сторона данного преступления состоит в нарушении правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей, повлекшем уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб. Предусмотренный комментируемой статьей состав преступления является материальным и его необходимым элементом является причинение крупного ущерба. Между фактом нарушения и наступившим ущербом должна быть установлена причинная связь. Наступившие последствия должны являться результатом нарушения правил эксплуатации, а не программной ошибкой либо действиями, предусмотренными в ст. ст. 272, 273 УК. Понятие крупного ущерба определено в примечании 1 к ст. 272 УК и должно составлять не менее одного миллиона рублей.

Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации, за которые предусмотрена ответственность данной статьей отличается от преступления, предусмотренного ст. 272 УК РФ тем, что виновный, в силу своего служебного положения, имеет право доступа к информации и является законным пользователем. То есть, субъект данного преступления – специальный.

Преступление может быть совершено и путем бездействия (например, не включать системы защиты информации, в результате чего наступают вредные последствия).

По данной статье редки случаи привлечение к уголовной ответственности из-за высокого материального порога состава преступления. Относится к преступлениям небольшой тяжести.

С 1 января 2018 года вступает в силу новая статья Уголовного Кодекса РФ – ст.274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации», которая вводится в соответствии с Федеральным законом № 194 –ФЗ от 26.07.2017.

По существу, новая норма уголовного закона содержит крайне схожее описание уголовно-наказуемых действий, закрепленных в диспозициях статей 272, 273 и 274 УК РФ, за исключением существенного отличия: объектом преступного посягательства является критическая информационная инфраструктура.

Одновременно принятием Федерального закона №187-ФЗ от 26.07.2017 года законодатель установил, что критическую информационную инфраструктуру РФ составляют объекты инфраструктуры в виде: информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления субъектами критической информационной инфраструктуры, а также сети электросвязи**,** используемые для организации взаимодействия таких объектов.

Другой отличительной особенностью статьи 274.1 УК РФ является ужесточение уголовной ответственности за совершение неправомерных действий вплоть до назначения безальтернативного наказания в виде лишения свободы от пяти до десяти лет.

Осуществлять расследование уголовных дел по статье 274.1 УК РФ уполномочена Федеральная служба безопасности Российской Федерации. В тоже время закон допускает возможность производства предварительного следствия следователями органа, выявившего подобное преступление (Следственный Комитет РФ, МВД РФ).

В России киберпреступность за последние три года выросла в шесть раз, сообщил генеральный прокурор России Ю.Я. Чайка. Такие данные он привел на встрече руководителей прокурорских служб государств БРИКС в Бразилии.

Ю. Я. Чайка отметил, что в России число преступлений, совершаемых с использованием современных информационно-коммуникационных технологий, с 2013 по 2016 г. увеличилось с 11 000 до 66 000. Значительный их рост наблюдается и в текущем году (+26%, 40 000).

При этом в Генпрокуратуре добавили, что помимо этого «всемирная сеть широко используется для пропаганды различных экстремистских идей и движений». Например, в 2016 г. в России две трети преступлений экстремистской направленности и каждое девятое преступление террористического характера совершались с использованием Интернета.

Кроме перечисленных ранее причин ненаказуемости за компьютерные преступления, существует несколько важных проблем.

1. Наибольшие трудности возникают при проведении осмотра места происшествия и назначении судебных экспертиз.

При этом многие респонденты отмечали, что и вовсе не проводили осмотр места происшествия. Причина проста – оно отсутствует. Это значит, что распознавание места совершения киберпреступления невозможно без установления обстановки совершения преступления, которая определяется системой киберпространства. Как уже говорилось ранее, основной особенностью киберпреступлений является трансграничность. То есть между преступником и жертвой могут быть тысячи километров. Для расследования преступлений, совершенных в киберпространстве, требуются как технические, так и теоретические знания.

2. Проведение экспертизы. Следователи отмечают высокую загруженность государственных судебно-экспертных учреждений и, как следствие, несвоевременностью выполнения экспертиз.
3. Немаловажной проблемой при назначении экспертиз является постановка грамотных вопросов эксперту. Назначающие экспертизу связывают возникающие трудности с отсутствием у них практики расследования данной категории дел, сложностью технических терминов и отсутствием специальных знаний в этой сфере.

В табл. 1 приводятся данные анализа материалов уголовных дел о киберпреступлениях [12].

Таблица 1. Данные анализа материалов уголовных дел о киберпреступлениях.

Следственные действия	%
1	2
Привлечение к осмотру места происшествия специалиста и эксперта-криминалиста.	91,7
По прибытии на место осмотра происшествия следователь запретил доступ к компьютерам и различным гаджетам (планшетные компьютеры, телефоны, смартфоны и прочее) всем лицам, находящимся на месте осмотра.	2,0
Выявление следов рук, оставшихся на компьютерной технике и периферийных устройствах.	41,7
Установление расположения всей компьютерной техники, в осматриваемом месте, места прокладки телекоммуникационных кабелей, наличие локальной, беспроводной (WI-FI) и глобальной сетей в помещении, наличие сервера.	16,7
Место происшествия осматривалось также на предмет запоминающих устройств.	58,3
Осмотрена документация и записи, относящиеся к киберпреступлениям.	16,7
Работающая компьютерная техника осматривается специалистом для выявления компьютерной информации, содержащей следы, совершённого киберпреступления.	75,0
Производится изъятие компьютерной техники и комплектующих.	50,0
Обыск проводился (да/нет).	30 / 70
Выемка техники проводилась (да/нет).	58.3 / 41.7
Предварительное получение достоверных данных: о виде и конфигурации используемой компьютерной техники; о подключении компьютерной техники к телекоммуникационным сетям; о наличии службы информационной безопасности и защиты от несанкционированного доступа; о системе электропитания помещений, где установлена компьютерная техника; о квалификации пользователей и другие.	16.7

Раскрытие и расследование киберпреступлений остается сложной задачей для сотрудников органов предварительного расследования. Это обусловлено:

- ✓ отсутствием системных обобщений материалов следственной и судебной практики;
- ✓ нехваткой методических рекомендаций по организации расследования данного вида преступлений;
- ✓ небольшим опытом работы конкретных следователей и работников органов дознания со специфическими источниками доказательственной информации, находящейся в электронной цифровой форме в виде электронных сообщений, страниц, сайтов;
- ✓ недостаточно высоким уровнем подготовки следователей по соответствующей специализации в высших учебных заведениях.

Так по данным [12] наибольшие трудности при расследовании киберпреступлений вызывают: допрос подозреваемого (71%); осмотр места преступления (42%).

В 69% причинами преступлений является корыстная заинтересованность; хулиганство в 10.5%, месть 9.3%, исследовательский интерес и самоутверждение - 12%.

Выводы

С развитием современных технологий сформировались условия к появлению нового вида преступлений, совершаемых в киберпространстве.

Этому новому виду преступности необходимо противопоставить действенные меры, в число которых входят и меры уголовно-правового воздействия.

Необходимо детальное изучение преступлений в сфере компьютерной информации для их правильной классификации и повышения эффективности борьбы с ними.

При расследовании киберпреступлений необходимы профессиональные знания, что обуславливает необходимость привлечения специалистов соответствующего профиля.

Необходима унификация уголовного законодательства различных государств, в т. ч. и Российской Федерации, предусматривающего уголовную ответственность за преступления в сфере компьютерной информации.

Литература

1. Доклад X Конгресса ООН по предупреждению преступности и обращению с правонарушителями // Право России. Режим доступа: http://portalus.ru/modules/russianlaw/rus_readme.php?subaction=showfull&id=1105644430&archive=old&start_from=&ucat=&.

2. Securitylab.ru by positive technologies. Российские компании сравнялись с

американскими по уровню кибербезопасности. Режим доступа: https://www.securitylab.ru /news/489586.php

3. Securitylab.ru by positive technologies. Путин поручил российским IT-компаниям перейти на отечественное ПО. Режим доступа: http://www.securitylab.ru/news/488380.php

4. Конвенция о компьютерных преступлениях. Режим доступа: https://www.coe.int/ru/web/conventions/full-list/-/conventions/rms/0900001680081580.

5. Informática Forense (Компьютерная криминалистика). Режим доступа: https://www.scoop.it/t/informatica-forense.

6. 70 ciberataques en diez días de grupos afines al independentismo. Режим доступа: https://politica.elpais.com/politica/2017/11/21/actualidad/1511286369_774264.html

7. Государство. Бизнес. ИТ. Киберпреступность в мире. Состояние киберпреступности в различных регионах мира. Режим доступа: http://www.tadviser.ru/index.php

8. Ассоциация электронных торговых площадок. Режим доступа: http://aetp.ru/market-news/item/395681

9. Киберпреступность — масштабы огромны, ответственности — ноль? Global CIO. Официальный портал IT - директоров. Режим доступа: http://www.globalcio.ru/theme-2011-03-first/

10. Николаева А.Б., Тумбинская М.В. Киберпреступность: история развития, проблемы практики расследования. Виртуальный компьютерный музей. Режим доступа: http://www.computer-museum.ru/articles/materialy-mezhdunarodnoy-konferentsii-sorucom-2014/629/

11. Уголовный кодекс Российской Федерации" от 13.06.1996 N 63-ФЗ (ред. от 29.07.2017) (с изм. и доп., вступ. в силу с 26.08.2017).

12. Шевченко Е.С. Тактика производства следственных действий при расследовании киберпреступлений. Диссертация на соискание учёной степени кандидата юридических наук, Москва, 2016.

Прикмета А. Н. Киберпреступность в России. Юридическая ответственность за нарушения прав в сфере информационных технологий. *Статья посвящена рассмотрению вопросов* ***к****иберпреступности в России. Дается анализ понятий «киберпреступность», «киберкриминальный рынок», оцениваются причины и особенности киберпреступлений. Особое внимание уделяется юридической ответственности за нарушения прав в сфере информационных технологий.*

Ключевые слова: *киберпреступность, киберкриминальный рынок, киберинциденты, ответственность за киберпреступления.*

Prikmeta A. N. Cybercrime in Russia. Legal liability for violations of rights in the field of information technology. *The article is devoted to the consideration of cybercrime in Russia. The analysis of the concepts "cybercrime", "cybercriminal market" is given, the causes and peculiarities of cybercrimes are estimated. Particular attention is paid to legal liability for violations of rights in the field of information technology.*

Keywords: *cybercrime, cybercriminal market, cyberincident, responsibility for cybercrime.*

Статья поступила в редакцию 21 мая 2018 г.
Рекомендована к публикации профессором Миненко А. С.

УДК 004.822:514

Кластеризация сообществ социальной сети «ВКонтакте»

И. Ю. Анохина, Е. В. Рощина
Донецкий национальный технический университет
Ingatula@mail.ru

Анохина И. Ю., Рощина Е. В. Кластеризация сообществ социальной сети «ВКонтакте». *Рассматриваются вопросы анализа социальных сетей. Проведен мониторинг и анализ тридцати восьми групп различных тематик, определены статистические показатели для оценки количественных и качественных характеристик участников групп. Проведена оценка уровня политизации групп. Проведен анализ существенности различий в личностных характеристиках участников сообществ различных групп. Методами кластерного анализа проведено разбиение групп на кластеры по уровню политизации.*

Ключевые слова: *социальные сети, ВКонтакте, кластерный анализ, структурные характеристики, мониторинг социальных сетей, политическая активность, политизация социальных сетей.*

Введение

Социальные сети прочно интегрировались в жизнь современного человека.

Теперь это не просто средство общения и связи, а полноценная медиакультура, в рамках которой обсуждаются новости, происходят продажи и покупки, рекламируются товары и формируется общественное мнение, это трибуны для политических партий и средство организации, координации сообщества, это площадки для раскручивания кампании и брендов.

Социальные сети можно классифицировать по типу: личное/деловое общение; видео/аудио/фото; развлечения; покупки/продажа; новости; тематические и многое другое.

Они могут быть открытыми и закрытыми, распространяться по всему миру, одной стране, региону или не зависеть от географии.

Социальную сеть можно рассматривать, как часть общества, на которую пытаются повлиять для достижения определенной цели. Это может быть формирование общественного мнения по определенному вопросу, а может использоваться при проведении маркетинга и бизнес - аналитики.

Для решения таких задач необходимо знать, каким образом максимально эффективно донести информацию до сообществ и их участников, определить максимально эффективные каналы распространения информации по сети, найти пользователей, готовых с большой вероятностью действовать в соответствии с разработанной доктриной.

Помимо формирования общественного в сети можно проводить оценку любого нововведения, будь то сервис, сообщество или рекламная компания. Такая оценка дает возможность разрабатывать сервисы не наугад, а целенаправленно повышать пользовательскую активность.

По мнению генерального директора «SECL Group» Н. Семенова более 80% компаний по всему миру использую социальные сети для развития бизнеса. Около 78% людей доверяют информации из социальных сетей[1].

Популярность сетей обуславливает необходимость в их изучении, анализе, моделировании.

Постановка задачи

Анализ социальных сетей стали применять во второй половине двадцатого века как дополнение к стандартному набору инструментов социальных исследователей.

Одним из первых направлений было исследование Social Network Analysis, рассматривающее социальные взаимосвязи в виде моделируемых графов и сетей. Модели строили на основе различных данных из печатных источников, дополнительных опросов и анкетирования.

Одной из главных тенденций современного развития сетей является их стремительная политизация. Уход в виртуальное пространство предполагает формирование различных сетевых политических сообществ со своими авторитетами и ценностями, причем среди них могут быть как провластные (патриотически-настроенные), так и оппозиционные (от конструктивных критиков до радикалов и экстремистов) [2].

Таким образом, социальные сети становятся не только неисчерпаемым источником бизнес – возможностей, но и источником риска для власти, включая

«цветные» революции и другие виды переворотов.

И, если сильно политизированной является, как правило, лишь незначительная часть общества, то используя социальные сети как инструмент, возможно привлечение все новых участников именно в политические группы. Как сказал античный философ Перикл: «Если Вы не интересуетесь политикой, то это не значит, что политика не интересуется Вами!»

Благодаря появлению социальных сетей стали публичными персональные данные участников сообществ, их биографии, аудио-, видео-, фотоматериалы, что сделало социальные сети отличным инструментом для получения информации как об отдельном индивидууме, так и группах лиц, объединенных общими интересами. Полученная информация используется для моделирования социальных, экономических политических и других процессов[3].

Как показали исследования, наиболее популярной социальной сетью в России является Вконтакте. Число пишущих авторов на лето 2017г. составило 27.5 млн. человек, основная возрастная группа – авторы в возрасте 25-34лет (37%), авторы женского пола составляют 58% . Наиболее популярной сеть является в Петербурге (44.9% от общего населения), на втором месте – Мурманская область (30%), Москва – 28% [4].

В 2016г. в России реализован научный проект – «Глобальное исследование политизации социальных сетей», в ходе которого анализировались интернет - сообщества стран Западной Европы, Северной Америки, Латинской Америки, Азии и Африки. Анализировался контент сообществ.

В Западноевропейском кластере наиболее политизированы Германия и Италия. В Германии наиболее многочисленны сообщества, выступающие против политики ЕС, за отставку Меркель и пр.

В США (Англосаксонский кластер), среди оппозиционных групп наиболее популярны группы, разжигающие ненависть между Севером и Югом. В то же время в Канаде популярны проправительственные группы, см. табл.1.

Интересен тот факт, что в Индии резко увеличивается число участников, вовлеченных в политические сообщества. Только за январь 2016г. количество подписчиков официального блога премьер-министра увеличилось практически на миллион.

Таблица 1. Политизация сообществ в социальных сетях

	Политические субкультуры		
Кластеры Интернета	провластная	оппозиционная	радикальная
Западноевропейский	38%	58%	*4%*
Англосаксонский	54%	33%	*13%*
Латиноамериканский	81%	18%	*1%*
Азиатский	59%	35%	*6%*
Африканский	41%	57%	*2%*

В социальных сообществах обсуждаются новости и события.

Появление оппозиционных и радикальных политизированных сообществ Интернета отчётливо видно на примере США («южане» и «северяне») и Германии.

Однако в таких странах, как Китай, Индия и Южная Корея интернет- сообщества служат поддержкой для власти.

Таким образом, как пишет известный испанский социолог Мануэль Кастельс, современная легитимность власти уже не может учитывать только силовые методы и заставляет власть искать новые сетевые приёмы для работы с электоратом.

Отсюда становится понятно значение современной виртуализации политической сферы и важность изучения этой части социальных сетей.

Мы исследовали российский кластер сообществ.

Для анализа выбрана социальная сеть ВКонтакте.

Чтобы оценить уровень политизации социальных сетей, возможности пересечения их участников, вероятность перемещения участников из одной группы в другую, мы рассматривали три типа сообществ.

1. Полностью **нейтральные** к политике группы по интересам (рыбалка, кулинарные рецепты, группы книголюбов, путешественников, любителей животных и пр.). Такие группы здесь и далее определены нами как «**группы по интересам**», при кластеризации отмечались как группы с

показателем **gr= -1**.

2. **Новостные** сообщества и сообщества, созданные для обсуждения политических новостей, сообщества партий, сообщества телеканалов, в целом дающие новости в позитивном плане, здесь и далее «**политические** группы», показатель **gr = 0**.
3. Третий вид групп аналогичен сообществам второго вида, но с ярко выраженной критической нотой, «**критики**», **gr = +1**.

Поставлена задача, провести статистический анализ участников сообществ с целью проведения кластеризации и выявления возможных тенденций миграции участников одного из видов сообществ к другому.

Исследования

Для решения задачи нами рассматривались 38 сообществ. По каждому сообществу анализировались данные, приведенные в табл.1.

Исследовали возраст, пол, город проживания и ряд других параметров, указанных в таблице.

Например, в столбце 2 таблицы указано, что 27.4% участников от общего числа в группе имеют возраст до 25 лет.

Данные исследовались в процентном отношении числа участников, соответствующих заданному критерию, к общему числу участников группы.

Номера столбцов в таблице соответствуют данным: 2- название группы, 3 – возраст до 25 лет, 4 – возраст от 25 до 35 лет, 5 – от 35 до 45; 6 – от 45 до 55; 7 – старше 55; 8 и 9 – количество женщин и мужчин в группе соответственно.

В столбцы 10 и 11 заносились процент участников, указавших в качестве религиозных взглядов православие (10) или светский гуманизм (11). На первом этапе обработки статистических данных мы рассматривали другие религии (буддизм, ислам…), но их процент был столь незначителен, что в дальнейшем оставили только два варианта.

Сообщество ВКонтакте предлагает участникам определить главное в жизни, выбирая из нескольких вариантов. В таблице эти варианты указаны в столбцах: 12 - совершенствование мира, 13 - семья и дети, 14- карьера и деньги, 15 – развлечения и отдых, 16 - наука и исследования, 17 – саморазвитие, 18 – красота и искусство, 19 – слава и влияние.

Нами на основании данных столбцов 3- 7 вычислялся средний возраст (столбец 20). Мы также ввели дополнительную характеристику, определив ее как степень открытости участников сообщества, оценив отношение количества заполненных анкет к общему числу участников сообщества (столбец 21).

Важным показателем реально функционирующего сообщества является процент ботов[2] (столбец 22) и активность подписчиков, определяемая как количество лайков, комментариев, репостов сообщений. (23). Эти показатели были определены с помощью on-line сервиса http://smmup.ru[6].

В табл. 2 приводятся выборочно данные по одной группе из каждого типа сообществ. Группа «Интересная планета» насчитывает более трех миллионов подписчиков, не содержит политической и новостной информации. Группа «Народный журналист» относится к группам критиков (около 6 тысяч подписчиков). «Первый канал» – более миллиона подписчиков.

Группы критиков имеют, как правило, незначительную численность. Самая большая по численности из проанализированных нами была группа «Сводки ополчения Новороссии», на момент анализа имеющая около полумиллиона подписчиков.

В группах по интересам преобладают женщины (42.4%), мужчины – 40.5%.

Политические группы в большей мере привлекают мужчин (50.1%) против 32.5% (женщины).

В группах критиков эта тенденция усиливается. 63.1% в группах – мужчины и 26.2: - женщины, т.е. количество мужчин-участников почти в три раза больше, чем женщин.

Как видим, не все участники сообществ указали свой пол. Немногим более 10% не дали ответ даже на этот вопрос.

С учетом этого нами и была введена характеристика открытости участников сообществ, т.е. их готовность предоставлять информацию о себе.

На рис.1. представлены гистограммы, отображающие распределение участников групп по возрастам (рис.1а) и характеристики непосредственно групп (процентное содержание ботов и активность посетителей в сутки), рис. 1б.

Анализируя данные по распределению возрастных категорий, следует отметить, что в группах по интересам преобладают молодые люди в возрасте до 25 лет, в то время, как в политических группах возрастная шкала смещена к 35 годам и старше.

[2] Боты - страницы Вконтакте, наполненные ложной информацией, либо, взломанные страницы реальных людей. Сферы применения : рассылка спама, накрутка подписчиков, лайков, репостов.

Таблица 2. Пример исходных данных для анализа сообществ

№	Группа	Возраст					Пол		Отноше-ние к религии		Главное в жизни								Дополнительные характеристики			
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23
1	Интерес-ная планета	27.4	44.4	11.2	3.4	3.4	50.5	33.6	14.5	0.7	1.3	13.5	0.7	1.0	0.2	5.2	0.6	0.2	30	23	13.5	1.1
2	Первый канал	31.4	28.7	12.1	5.6	6.5	49.8	31.7	12.3	0.5	1.0	13.3	0.8	0.8	0.3	3.4	0.6	0.2	32	20	13.4	0.38
3	Народ-ный журна-лист	7.5	24.7	29.1	17.3	16.3	31.6	58.6	14.5	3.3	5.8	9.9	0.5	0.4	0.9	8.1	0.9	0.5	42	27	6.50	19.7

В группах критиков во всех возрастных категориях старше 35 количество участников превышает аналогичные показатели в остальных видах групп.

Минимальное количество ботов и активность подписчиков в сутки(8%) в группах, критиков, что более, чем в два раза превышает активность в остальных видах групп.

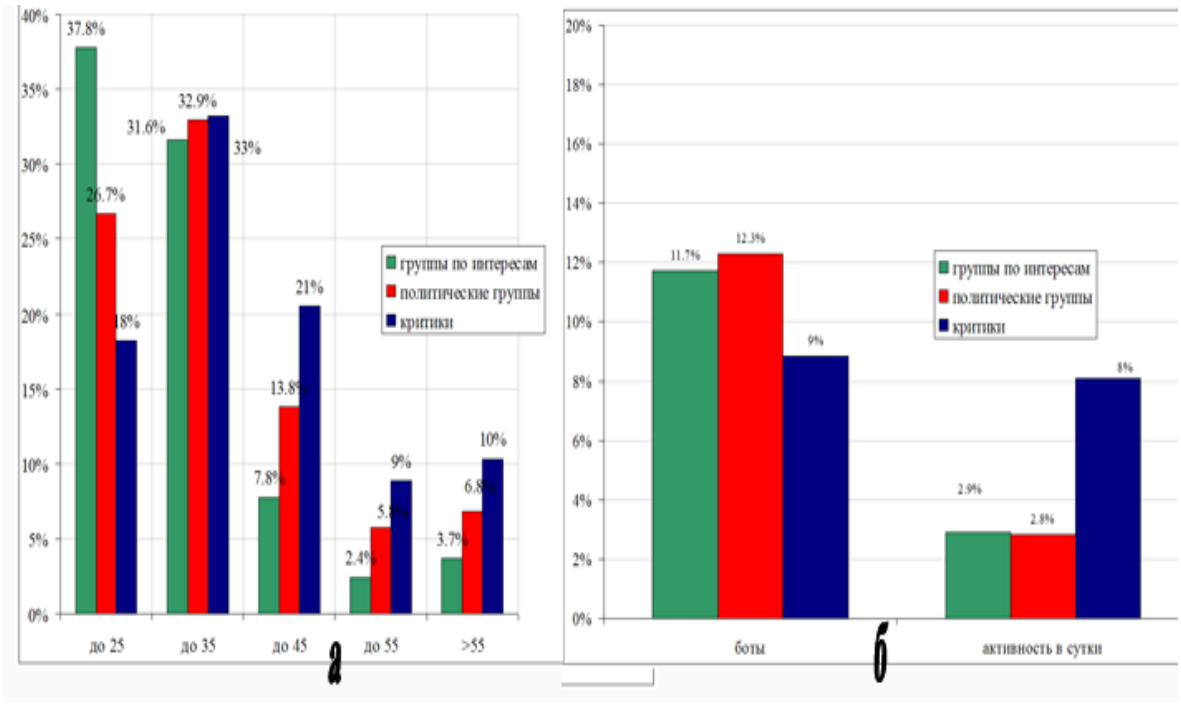


Рисунок 1 – Количественные характеристики групп. а – распределение по возрастному признаку; б – активность участников групп

В целях оценки существенности различий между группами в среде пакета Statistica был проведен t – тест с уровнем значимости p=0.05. В табл.3 приведены результаты тестирования.

Для всех групп рассчитывались значения математического ожидания (столбцы 1, 2, 5, 6, 9, 10), определялась величина коэффициента Стьюдента (t-value) и уровень значимости p.

Как видно из таблицы, наличествуют существенные различия по одиннадцати характеристикам между контингентом групп по интересам и участниками групп-критиков (выделены красным).

Состав участников политических групп и групп по интересам отличается в меньшей степени и только по шести признакам, в основном связанным с возрастом и отношением к религии.

Наиболее существенно различаются политические группы и группы –критики (четырнадцать позиций).

Таким образом, первичная обработка данных позволила сделать вывод о наличии существенных различий между контингентом анализируемых групп.

Таблица 3. Т- тест определения существенности различий между выборками данных

Сравнение групп по интересам и групп-критиков					Сравнение групп по интересам и политических групп				Сравнение групп-критиков и политических групп			
	1	2	3	4	5	6	7	8	9	10	11	12
	gr=-1	**gr=1**	t-value	p	**gr=-1**	**gr=0**	t-value	p	**gr=1**	**gr=0**	t-value	p
До 25	**0.38**	**0.18**	**3.62**	**0.00**	**0.38**	**0.27**	**2.25**	**0.03**	**0.18**	**0.27**	**-3.05**	**0.01**
До 35	0.32	0.33	-0.45	0.66	0.32	0.33	-0.36	0.72	0.33	0.33	0.15	0.89
До 45	**0.08**	**0.21**	**-6.03**	**0.00**	**0.08**	**0.14**	**-4.75**	**0.00**	**0.21**	**0.14**	**3.20**	**0.00**
До 55	**0.02**	**0.09**	**-4.89**	**0.00**	**0.02**	**0.06**	**-5.73**	**0.00**	**0.09**	**0.06**	**2.29**	**0.03**
Старше 55	**0.04**	**0.10**	**-7.57**	**0.00**	**0.04**	**0.07**	**-4.83**	**0.00**	**0.10**	**0.07**	**3.52**	**0.00**
Ж	**0.42**	**0.26**	**2.71**	**0.01**	0.42	0.33	1.57	0.13	0.26	0.33	-1.57	0.13
М	**0.41**	**0.63**	**-3.45**	**0.00**	0.41	0.50	-1.44	0.16	**0.63**	**0.50**	**3.24**	**0.00**
Православие	0.12	0.14	-1.96	0.06	**0.12**	**0.16**	**-3.56**	**0.00**	0.14	0.16	-1.22	0.23
Светский гуманизм	**0.01**	**0.03**	**-5.74**	**0.00**	**0.01**	**0.01**	**-2.60**	**0.02**	**0.03**	**0.01**	**3.57**	**0.00**
Совершен-ствование мира	**0.01**	**0.07**	**-3.24**	**0.00**	0.01	0.02	-1.59	0.13	**0.07**	**0.02**	**2.66**	**0.01**
Семья и дети	0.16	0.14	0.48	0.63	0.16	0.14	0.55	0.59	0.14	0.14	-0.11	0.91
Карьера	0.01	0.01	0.11	0.92	0.01	0.01	-0.03	0.98	0.01	0.01	-0.20	0.84
Отдых	0.02	0.01	1.24	0.23	0.02	0.01	1.57	0.13	0.01	0.01	0.29	0.77
Наука	**0.00**	**0.01**	**-4.22**	**0.00**	0.00	0.00	-0.97	0.34	**0.01**	**0.00**	**2.97**	**0.01**
Самораз-витие	**0.05**	**0.09**	**-3.16**	**0.00**	0.05	0.05	-0.10	0.92	**0.09**	**0.05**	**3.54**	**0.00**
Искусство	0.01	0.01	-0.47	0.64	0.01	0.01	1.51	0.15	**0.01**	**0.01**	**3.19**	**0.00**
Слава	**0.00**	**0.01**	**-3.28**	**0.00**	0.00	0.00	-1.41	0.17	**0.01**	**0.00**	**2.12**	**0.05**
Открытость	0.83	0.90	-1.95	0.06	0.83	0.84	-0.31	0.76	**0.90**	**0.84**	**3.17**	**0.00**
Боты	0.13	0.09	1.99	0.06	0.13	0.12	0.24	0.81	**0.09**	**0.12**	**-2.28**	**0.03**
Активность	0.04	0.08	-1.75	0.09	0.04	0.03	0.71	0.49	**0.08**	**0.03**	**2.34**	**0.03**

Анализируя выборки, состоящие из нескольких групп, мы доказали наличие существенных различий, но в выборках в целом. В то же время нельзя исключать, что отдельные группы, входящие допустим в выборку по интересам, не могут быть по характерным признакам отнесены к той или иной политической группе.

Вряд ли можно утверждать, что люди, вступившие в группу, допустим, путешественников, книголюбов, никогда не интересовались политикой и не будут интересоваться ею впредь.

Поэтому далее нами был применен кластерный анализ с целью выявления возможных тенденций миграции или добавления участников одной выборки в другую.

При проведении кластерного анализа рассматривалась возможность наличия от трех до шести кластеров, на которые могла быть разбита вся выборка, состоящая из 38 групп. В качестве переменных использовались все переменные, указанные в табл.1. за исключением тех, в которых не были зафиксированы существенные различия между группами.

На первом этапе кластерного анализа определялось оптимальное число кластеров. Для этого использовали метод иерархического

кластерного анализа Joining (Tree clustering). В качестве метрики, определяющей расстояние между кластерами Amalgamation Rule, был выбран метод ближнего соседа или одиночная связь (single linkage)[7,8]. На рис.2. показана часть обработанных кластеров.

CLUSTER ANALYSIS	Single Linkage Euclidean distances					
linkage distance	Obj. No. 1	Obj. No. 2	Obj. No. 3	Obj. No. 4	Obj. No. 5	Obj. No. 6
.0828254	x_6	x_8				
.0898790	x_33	x_34				
.0916961	x_31	x_37				
.0938040	x_17	x_23				
.0948636	x_17	x_23	x_20			
.0951687	x_31	x_37	x_33	x_34		
.0958407	x_24	x_25				
.1023266	x_18	x_31	x_37	x_33	x_34	
.1089584	x_28	x_36				
.1135806	x_6	x_8	x_28	x_36		
.1292735	x_26	x_38				
.1294454	x_24	x_25	x_26	x_38		
.1325940	x_5	x_30				
.1415378	x 5	x 30	x 24	x 25	x 26	x 38

Рисунок 2 – Матрица расстояний между центрами кластеров

Как видно из рис.2, на первом этапе в один кластер объединяются объекты с номерами 6 (группа «Путешествия и туризм) и 8 («Интересная планета»). Ясно, что люди, склонные к путешествиям, не могут не интересоваться планетой, географией и пр.

В другой кластер попадают группы 31(КПРФ – Коммунистическая партия РФ), 33 («Вежливые люди»), 37 – «Телеканал Звезда».

Аналогичным образом нами были проанализированы остальные составляющие кластеров.

На основании анализа было принято решение разделить группы на пять кластеров. Для определения, какие именно группы входят в кластеры, был применен метод k-средних (**k**-means). Суть метода состоит в следующем: заранее определяют количество классов (**k**), на которые необходимо разбить имеющиеся наблюдения, и первые **k** – наблюдений становятся центрами этих классов. Для каждого следующего наблюдения рассчитываются расстояния до центров кластеров и анализируемое наблюдение относят к тому кластеру, расстояние до которого было минимальным. После чего для этого кластера (в котором увеличилось количество наблюдений) рассчитывается новый центр тяжести по всем включенным в кластер наблюдениям. Показателем правильности разбиения на кластеры является выводимая таблица расчета дисперсий и уровня значимости p (см. табл.4).

Таблица 4. Таблица анализа дисперсий

Показа-тели	Возраст					Пол		Характеристики группы		
	<25	<35	<45	<55	>55	Ж	М	открытость	боты	активность
Between SS	0.43	0.05	0.13	0.04	0.03	0.64	0.89	0.072	0.018	0.043
Within SS	0.26	0.16	0.04	0.02	0.01	0.21	0.20	0.169	0.063	0.071
F	13.81	2.57	24.68	20.14	18.45	25.77	36.98	3.531	2.405	5.038
p	**0.00**	0.05	**0.00**	**0.00**	**0.00**	**0.00**	**0.00**	**0.017**	0.049	**0.003**

В таблице приняты обозначения: дисперсия между кластерами **Between SS**, дисперсия внутри кластеров (**Within SS**), **F**-критерий для проверки гипотезы о неравенстве дисперсий F, значение уровня **p** [9].

Как следует из анализа данных табл.3, можно считать достоверным предложенное разбиение на кластеры. Уровень p только для одной возрастной группы (от 25 до 35) достигает критического значения 0.05 и для характеристики, связанной с наличием ботов в группах, равен 0.049, т.е. приближается к критическому значению.

Аналогично оценили степень достоверности по критерию Фишера. Следовательно, мы можем принять и считать

допустим предложенное деление на кластеры.

На рис. 3 дана графическая интерпретация полученного деления на кластеры. Как видно из рисунка, наиболее существенное деление в кластерах происходит по возрастному, половому признакам и по степени активности участников групп.

Отметим, что участники всех групп в качестве основной составляющей жизни указывали семью. Совершенствованием мира готовы заниматься в пять раз больше участников групп-критиков, чем участники остальных групп. Эта же группа отличается стремлением к самосовершенствованию и тяге к научным исследованиям. А вот карьеру и деньги в качестве основной цели назвали участники политических групп (gr=0).

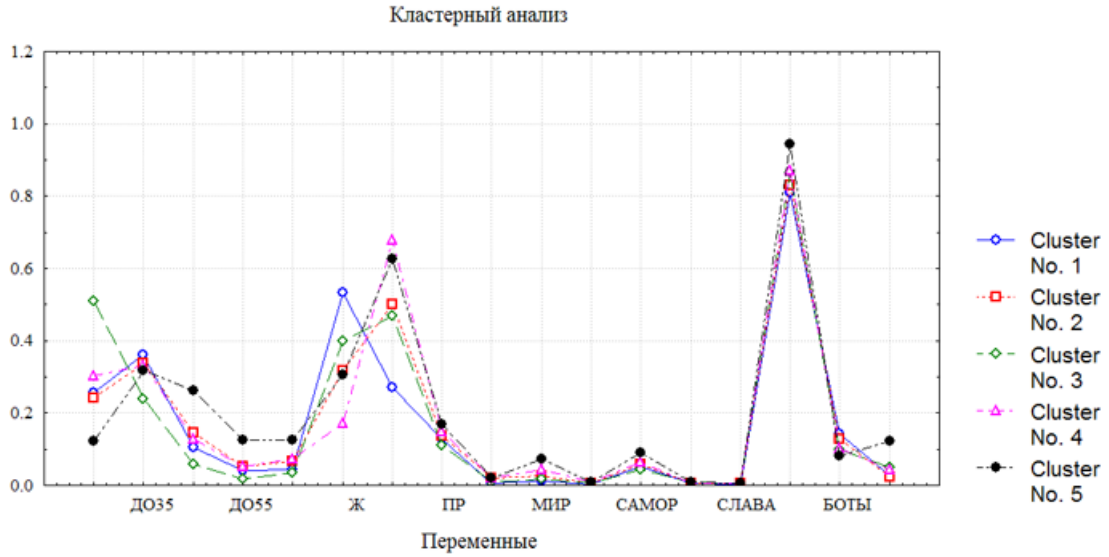


Рисунок 3 – Средние значения переменных для каждого кластера

На основании расчетов и анализа данных следующим образом произведено распределение по кластерам:

1. В первый кластер вошли группы, созданные для лиц, увлекающихся путешествиями, географией, здоровьем, домашними животными и домашним хозяйством. Все эти группы были отмечены у нас как группы по интересам. В этот же кластер вошли группы «Первый канал», «Типичный Донецк» и «Donbass.media Group». Т.е. первый кластер объединил участников без видимого интереса к политике, что показывает и то, что перечисленные три группы, определенные нами ранее как политические, в полной мере таковыми не являются.
2. Во второй кластер вошли группы, которые мы определили как созерцателей. Это группа «Киномания», «Discovery», «Интересная планета», «Бумажный самолетик». Во всех группах, как правило, размещаются красивые фотографии, описания интересных мест. Все перечисленные группы входили в группы по интересам.
3. В третий кластер вошли наиболее остро критикующие группы: «Сводки ополчения Новороссии», «Хроника вставания с колен», «Злюкен Енотен», «Еноты Новороссии», «Очищение», «Народный журналист». Ранее все группы были отнесены к группам критиков.
4. В четвертый кластер вошли группы «Оппозиция», КПРФ, ЛДПР, «Высокие технологии», «Рыбалка», «Преступная Россия», «Другая Россия», «Левый фронт». Отметим, что в этот кластер вошли, как нейтральные группы, так и группы –критики и политические группы. Группы «Другая Россия», «Левый фронт» считаются группами оппозиционных партий.
5. В пятый кластер вошли группы «Единая Россия», «Народное ополчение Павла Губарева», «Донецкая республика», «Комсомольская правда», «МИД России», «Луганск. Новости ЛНР», «Политика», «Права человека», это группы политические, воспринимающие все в позитивном ракурсе.

Можно сделать вывод, что в целом рассмотренный контингент участников делится на пять кластеров. Кластер сообществ абсолютно индифферентных к политике (кластер 2); кластер лиц имеющих свои увлечения и предпочитающих получать краткие политические новости (кластер 1). Кластер критикующих (кластер 3) и два кластера политической направленности, причем в одном из них в группы выкладываются только позитивные новости (кластер 5), в другом возможна незначительная критика (кластер 4).

Общее количество участников во всех проанализированных группах более 33млн. чел. Как видно из табл.5, почти 90% сообщества не

интересуются политическими темами, 1.24% критикуют происходящие события, 9% политикой интересуются, но в целом их устраивает текущее положение дел.

Таблица 5. Процентное соотношение кластеров

Кластер	Группы по интересам	Созерцатели	Критики	Нейтральные группы, критики, позитивные группы	Позитивные группы	Количество участников
№	1	2	3	4	5	
Участники	1 2416 300	16 972 105	411 020	2 148 030	1 199 613	33 147 068
%	37.46%	51.2%	1.24%	6.28%	3.62%	100%

Полученные данные не противоречат данным других источников [10,11]. Как правило, политически активными является лишь незначительная (до 10%) часть общества, однако, как показывают исследования, политическая активность населения растет [12].

Отметим, что если участники второго кластера не имеют склонности к обсуждению политических новостей, то вошедшие в третий кластер сообщества могут стать политизированными или уже являются ими, а значит могут перейти или в разряд позитивных, проправительственных групп или стать оппозицией.

Выводы

Политизация социальных сетей делает важным вопрос их изучения именно с точки зрения поддержки или отрицания власти.

В 2010 году в США блогосфера признана самостоятельным направлением реализации внешней политики США, что подчеркивает важность роли Интернета и необходимости активного присутствия в нем политических партий и организаций [13].

Чтобы побеждать в информационной войне необходимо выстраивать многомерные сети на основе информационных, культурных, политических и других компонентов.

Чтобы выстраивать такие сети, необходимы разработки моделей сообществ, изучения личностных характеристик их участников, необходимы моделирование их поведения и прогнозирования тенденций вовлечения нейтральных, неполитизированных членов сообществ в политические группы.

Литература

1. SECL Group. Н. Семенов. Все о социальных сетях. Влияние на человека. Режим доступа: https://secl.com.ua/article-vse-o-socialnyh-setjah-vlijanije-na-cheloveka.html

2. Федорченко С.Н. Глобальное исследование политизации социальных сетей // Обозреватель -Observer, 2016. №8(319). С. 57-67.

3. Тематическая классификация сообществ в социальной сети «ВКонтакте» как нового средства массовой информации. Морозова А.А.: Сборник Сучасная медыясфера: практыка трансфармацыі, тэарэтычнае асэнсаванне, інстытуцыянальныя перспектывы матэрыялы I Міжнароднай навукова-практычнай канферэнцыі. С. В. Дубовік (адказны рэдактар). 2017. С. 160-166.

4. Brand Analytics. Социальные сети в России, лето 2017: цифры и тренды. Режим доступа: http://blog.br-analytics.ru/sotsialnye-seti-v-rossii-leto-2017-tsifry-i-trendy/

5. Мануэль Кастельс. Информационная эпоха: экономика, общество и культура. - ГУ ВШЭ, 2000.-608с.

6. Анализ сообществ. On-line сервис Smmup.ru. Режим доступа: http://smmup.ru/activity.php

7. Боровиков В.П., Боровиков И.П. STATISTICA. Статистический анализ и обработка данных в среде Windows. - М.: Филинъ, 1998.- 608с.

8. Боровиков В.П. Популярное введение в современный анализ данных в системе STATISTICA. -М.: Горячая линия, 2016. -288с.

9. Statsoft. Электронный учебник по статистике. Режим доступа: http://statsoft.ru

10. Вайдлих. Социодинамика: системный подход к математическому моделированию в социальных науках.- М.: Едиториал, 2004. - 480с.

11. Манипуляция обществом или истинный размер пяти процентов. Режим доступа: https://alex-leshy.livejournal.com/480772.html

12. Рощина Е.В., Анохина И.Ю. Жизненный цикл групп в социальных сетях/Информатика, управляющие системы, математическое и компьютерное моделирование в рамках III форума «Инновационные перспективы Донбасса» (ИУСМКМ – 2017): VIII Международная научно-техническая конференция, 25 мая 2017, г. Донецк: / Донец. национал. техн. ун-т; Донецк: ДонНТУ, 2017, с. 73-77.

13. Филимонов Г., Градосельская Г. Поле битвы — соцсети. Особенности нынешней информационной войны. Режим доступа: http://svpressa.ru/society/article/147378/

Анохина И. Ю., Рощина Е. В. Кластеризация сообществ социальной сети «ВКонтакте». *Рассматриваются вопросы анализа социальных сетей. Проведен мониторинг и анализ тридцати восьми групп различных тематик, определены статистические показатели для оценки количественных и качественных характеристик участников групп. Проведена оценка уровня политизации групп. Проведен анализ существенности различий в личностных характеристиках участников сообществ различных групп. Методами кластерного анализа проведено разбиение групп на кластеры по уровню политизации.*

Ключевые слова: *социальные сети, ВКонтакте, кластерный анализ, структурные характеристики, мониторинг социальных сетей, политическая активность, политизация социальных сетей.*

I. Yu. Anokhina, E. V. Roshchina. Analysis of communities in social networks. *The analysis of social networks on the example of the social network "VKontakte" is considered. The example of thirty-eight groups of different subjects identified statistical indicators to assess the quantitative and qualitative characteristics of groups. Groups of three types were considered: apolitical groups, groups of political orientation without a critical component and a group of critics whose participants criticized the majority of the events under consideration. A t-test of communities was carried out, the presence of significant differences between the contingent of groups was revealed. By cluster analysis methods, all groups are divided into clusters, composition and percentage of clusters are determined, their characteristics are analyzed. The percentage of clusters that characterizes the degree of politicization of communities is determined.*

Keywords: *social networks, VKontakte, cluster analysis, structural characteristics, monitoring of social networks, political activity, politicization of social networks.*

Статья поступила в редакцию 15 мая 2018 г.
Рекомендована к публикации профессором Павлышом В. Н.

УДК 004.89

Перспективы и сложности развития искусственного интеллекта

Е. В. Лапшина, К. Н. Ефименко
Донецкий национальный технический университет
Kat_Lapshina@mail.ru, KN_Efimenko@mail.ru

Лапшина Е. В., Ефименко К. Н. Перспективы и сложности развития искусственного интеллекта. *Рассматривается история развития искусственного интеллекта, проблемы его разработки, современные тенденции и направления в развитии, основные области практического применения.*

Ключевые слова: *искусственный интеллект, история развития, проблемы разработки, практическое применение.*

Введение

В последнее время в научном мире все больше высказывается опасений в связи с развитием искусственного интеллекта. В октябре 2017г. британский физик с мировым именем Стивен Хокинг заявил, что искусственный интеллект не только может превзойти людей, но и заменить человечество как вид разумной жизни, проживающей на Земле. С аналогичными опасениями выступили Илон Маск (мультимиллиардер, исследователь-филантроп и глава SpaceX и Tesla) и Мустафа Сулейман (создатель искусственного интеллекта для Google). В августе 2017 г. они в составе группы экспертов в области робототехники и искусственного интеллекта, состоящей из 116 человек из 26 стран, обратились к ООН с призывом запретить разработку и использование автономного летального оружия (терминаторов).

Целью данной работы является попытка отследить современные тенденции и направления в развитии искусственного интеллекта, описать наиболее перспективные области его применения и определить, какую опасность он может представлять для человечества.

История развития искусственного интеллекта

В Википедии понятие «Искусственный интеллект» (*Artificial intelligence*) определяется двояко: как наука и технология создания интеллектуальных машин и компьютерных программ; и свойство интеллектуальных систем выполнять творческие функции, которые традиционно считаются прерогативой человека [1]. Таким образом, искусственный интеллект (ИИ) можно определить как область компьютерной науки, занимающуюся автоматизацией разумного поведения [2].

В целом, искусственный интеллект – это самостоятельная область научных исследований, которая сформировалась в результате достижений в математике и логике и основана на накопленных человечеством знаниях о живой и неживой природе [3].

Истоки возникновения ИИ можно отследить, начиная со средних веков, когда в понятие искусственного интеллекта вкладывали задачи создания механической человекоподобной мыслящей машины, способной, возможно, превзойти его по интеллекту.

В XVIII в. благодаря развитию техники и, в особенности, часовых механизмов интерес к подобным изобретениям вырос ещё сильнее. В середине 1750-х годов австрийский изобретатель Фридрих фон Кнаус, сконструировал серию машин, умевших писать пером довольно длинные тексты. В 1914 году директор одного из испанских технических институтов Леонардо Торрес Кеведо изготовил электромеханическое устройство, способное разыгрывать простейшие шахматные эндшпили почти также хорошо, как и человек [3].

В XIX в. целью создания формального языка для описания мышления задался математик Джордж Буль. Наиболее известным его открытием стала математическая формализация законов логики, в дальнейшем получившая название «Булева алгебра». Работа Буля стала базой для последующего развития формальной логики, включая разработку современных компьютеров. При этом цели самого Буля при разработке его системы по духу были ближе к современному ИИ.

В XX в. одной из первых работ, посвященных вопросу о машинном разуме в отношении современных цифровых компьютеров, стала статья «Вычислительные машины и интеллект», написанная в 1950 г. британским математиком Аланом Тьюрингом [4]. Тьюринг рассмотрел вопрос о том, можно ли заставить машину действительно думать. Отмечая, что фундаментальная неопределенность в самом вопросе (что такое

«думать»? и что такое «машина»?) исключает возможность рационального ответа, он предложил заменить вопрос об интеллекте более четко определенным эмпирическим тестом. Тест Тьюринга (рис.1) сравнивает способности предположительно разумной машины со способностями человека – лучшим и единственным стандартом разумного поведения.

В тесте, который Тьюринг назвал «имитационной игрой», машину и ее человеческого соперника помещают в разные комнаты, отделенные от комнаты, в которой находится экзаменатор. Экзаменатор не должен видеть их или говорить с ними напрямую – он общается с ними исключительно с помощью текстового устройства, например, компьютерного терминала. Экзаменатор должен отличить компьютер от человека исключительно на основе их ответов на вопросы, задаваемые через это устройство. Если же экзаменатор не может отличить машину от человека, тогда, утверждает Тьюринг, машину можно считать разумной [2a]. Таким образом, Тьюринг спрашивает, может ли машина совершать действия, неотличимые от обдуманных действий. Такая постановка вопроса позволяет избежать философских проблем по определению глагола «думать» и сосредоточить внимание на задачах создания и увеличения производительности, которая делает способность думать возможной [1].

Рисунок 1 – Тест Тьюринга

В нашей стране направление «Искусственный интеллект» возникло с опозданием примерно на 10 лет и пришло на смену кибернетическому и бионическому буму первой половины 60-х годов XX века. Практически с самого начала учёные, занимавшиеся этим новым направлением научных знаний, предположили, что к конструктивному определению и моделированию мышления полезно идти от специфики задач, вводя искусственный интеллект как механизм, необходимый для их решения. Таким образом, искусственный интеллект в современном понимании – это совокупность методов и инструментов решения различных сложных прикладных задач, использующих принципы и подходы, аналогичные размышляющему над их решением человеку или процессам, протекающим в живой или неживой природе [2].

На сегодняшний день исследования в области искусственного интеллекта ведутся по различным направлениям: представление знаний, моделирование рассуждений, приобретение знаний, машинное обучение и автоматическое порождение гипотез, интеллектуальный анализ данных и обработка образной информации, поддержка принятия решений, управление процессами и системами, динамические интеллектуальные системы, планирование и т.д. [3].

Сложности разработки искусственного интеллекта

Перед разработчиками ИИ стоит две наиболее фундаментальные проблемы – *представление знаний* (knowledge representation) и *поиск* (search). Первая относится к проблеме получения всего спектра новых знаний, требуемых для формирования разумного поведения, с помощью формального языка, подходящего для компьютерных манипуляций. Вторая – это метод решения проблемы, в котором систематически просматривается пространство *состояний задачи* (problem states), т.е. альтернативных стадий ее решения. По утверждению Ньюэлла и Саймона, высказанному в 1976 г., эта техника лежит в основе человеческого способа решения различных задач [2].

В тоже время все возможности современного компьютера определяются тремя факторами [5]:

1) разнообразие видов данных, которые могут быть представлены в числовом виде;

2) постоянное увеличение быстродействия;

3) увеличение производительности за счет распараллеливания вычислений.

Массовое внедрение компьютеров во все сферы деятельности человека сформировало некоторые причины, побудившие развитие исследований в области искусственного интеллекта:

– необходимость приблизить компьютеры к непрограммирующему пользователю, сделать общение с ним столь несложным, чтобы научиться этому при желании мог каждый человек без особых усилий;

– возникновение новых информационных технологий, при создании которых имеют значение не только результаты развития вычислительной техники и сетей связи, но и достижения искусственного интеллекта, без которых невозможна формализация и передача

знаний, манипулирование знаниями и доступ к ним;

– появление роботизированной техники способной избавить от лишних производственных затрат. Однако, для того чтобы полностью заменить человека, машина должна обладать достаточно высоким уровнем интеллекта, чтобы иметь возможность решать сложные производственные задачи. Прежде всего, это задачи зрительного восприятия, планирования целесообразного поведения, овладение навыками.

Основная проблема, стоящая перед исследователями и разработчиками искусственного интеллекта, состоит в рациональности применения достижений ИИ-разработок. Особую опасность представляют новшества военного вооружения и стратегии. К примеру, методы распознавания образов нашли свое применение при разработке крылатых ракет. Подобным образом и другие методы ИИ могут сыграть свою роль в военных системах будущего, способных планировать свои действия без участия людей. И, наконец, стоит отметить, что широкое внедрение информационных и экспертных систем может привести к появлению своеобразных «интеллектуальных тунеядцев», полностью доверяющих машине и стремящихся избавиться от необходимости прилагать малейшие интеллектуальные усилия. [2]

Основные области практического применения искусственного интеллекта

Современные работы в области практического применения искусственного интеллекта ведутся по нескольким основным направлениям [3]:

1. Распознавание зрительных или звуковых образов, а также других (смешанных) модальностей. Медицинская диагностика, предсказание погоды являются примерами задач распознавания образов. В последнее время основная часть работ в этой области ориентирована на анализ ситуаций (сцен), а не отдельных объектов (например, печатных знаков).

2. Использование естественного языка подразумевает разработку систем «вопрос-ответ» и систем автоматического перевода.

3. Экспертные системы, воплощающие большие объемы знаний и навыков, присущих эксперту – человеку. Эти системы представляют большую ценность, в частности, в медицинской диагностике, в геологии, а также в некоторых других областях.

4. Инженерия знаний хоть и не является самостоятельной областью, но сам термин отражает определенное отношение к тому, каким образом следует осуществлять взаимодействие различных видов знаний в распознавании образов, робототехнике и в экспертных системах. Также включает область, в рамках которой ведутся исследования по определению знаний, манипулированию ими и слежению за пополнением и корректировкой знаний.

5. Моделирование игр является основой для изучения эвристического поиска. Программы ведения игр ставят перед исследователями новые вопросы, включая вариант, при котором ходы противника невозможно определенно предугадать. Наличие противника усложняет структуру программы, добавляя в нее элемент непредсказуемости и потребность уделять внимание психологическим и тактическим факторам игровой стратегии.

6. Доказательство теорем перекрывается с определенными областями математики и решением проблем в ряде других областей (например, в робототехнике).

7. Нейронные сети. В эту область исследований входят такие перспективные методы, как обработка видеоизображений и их преобразование в векторные графические модели, автоматизация построения и анализа объектов моделей или местности с учетом динамики их развития, получение аналитических решений в графическом виде в режиме реального времени, работа с зашумленными данными и др. Например, в экономике для предсказания рынков, оценки риска невозврата кредитов, предсказания банкротств, оптимизации товарных и денежных потоков, автоматического считывания чеков и форм. В медицине: обработка медицинских изображений, мониторинг состояния пациентов, диагностика, факторный анализ эффективности лечения, очистка показаний приборов от шумов. В авиации: обучаемые автопилоты, распознавание сигналов радаров, адаптивное пилотирование сильно поврежденного самолета. В средствах связи: сжатие видео-информации, быстрое кодирование-декодирование, оптимизация сотовых сетей и схем маршрутизации пакетов.

8. Генетические алгоритмы позволяют исследователям вырабатывать новые решения проблем из компонентов предыдущих решений. Генетические операторы, такие как скрещивания или мутация, подобно своим эквивалентам в реальном мире, вырабатывают с каждым поколением все лучшие решения.

9. Языки программирования и среды разработки программного обеспечения ИИ являются одними из наиболее важных побочных продуктов исследований ИИ. По множеству причин, включая размеры многих прикладных программ ИИ, важность методологии “создания прототипов”, тенденцию алгоритмов поиска порождать чересчур большие пространства и трудности в предсказании поведения

эвристических программ, программистам искусственного интеллекта пришлось разработать мощную систему методологий программирования. Средства программирования включают такие методы структурирования знаний, как объектно-ориентированное программирование и каркасы экспертных систем. Высокоуровневые языки, такие как LISP и PROLOG, которые обеспечивают модульную разработку, помогают управиться с размерами и сложностью программ. Пакеты средств трассировки позволяют программистам реконструировать выполнение сложного алгоритма и разобраться в сложных структурах эвристического перебора. Без подобных инструментов и методик вряд ли удалось бы построить многие известные системы ИИ. [2]

10. Машинное обучение является одним из направлений искусственного интеллекта. Основной принцип заключается в том, что машины получают данные и «обучаются» на них. В настоящее время это наиболее перспективный инструмент для бизнеса, основанный на искусственном интеллекте. Системы машинного обучения позволяют быстро применять знания, полученные при обучении на больших наборах данных, что позволяет им преуспевать в таких задачах, как распознавание лиц, распознавание речи, распознавание объектов, перевод, и многих других. В отличие от программ с закодированными вручную инструкциями для выполнения конкретных задач, машинное обучение позволяет системе научиться самостоятельно распознавать шаблоны и делать прогнозы. Так программа DeepMind, разработанная ИИ-подразделением Google и являющаяся примером использования машинного обучения, обыграла чемпиона мира по Го, обучая себя на большом наборе данных ходов, сделанных опытными игроками [6].

11. Робототехника – это область исследований, которая ставит перед собой цель вывести машины из вычислительных центров в реальный мир [2].

В настоящее время практическими исследованиями в области ИИ занимаются такие ведущие мировые научные центры:

1. Лаборатория искусственного интеллекта в Университете Мичигана. Основная специализация – исследования и разработка вспомогательных технологий для лиц с физическими и когнитивными нарушениями. Один из таких проектов – разработка компьютерного интерфейса, автоматически приспосабливаемого к нуждам лиц с нарушением зрения.

2. Совместный исследовательский центр Стэндфордской лаборатории искусственного интеллекта и Toyota проводят исследования в области создания «умных» автомобилей следующего поколения. Разработки объединили специалистов в таких отраслях, как машинное обучение, роботехника и обработка естественного языка.

3. Группа искусственного интеллекта Кембриджского университета охватывает несколько дисциплин – включая геномику, теорию вычислительного обучения и нечеткую логику – и призвана разрабатывать эффективные алгоритмы, решающие проблемы машинного распознавания шаблонов и выявлять практические приложения таких моделей [7].

Перспективы развития искусственного интеллекта

Специалисты в области исследования и разработки искусственного интеллекта прогнозируют следующие перспективы развития и внедрения ИИ в жизнь [8].

1. В большинстве областей экономической и социальной жизни будет активно моделироваться поведение людей, основанное на их персональных данных.

2. С ростом глобальных сетей большинство окружающих нас гаджетов будут контактировать друг с другом и делать свою работу на основе алгоритмов ИИ.

3. С ростом доступности 3D-технологий производство станет не только штучным, но и персонализированным, смоделированным на основе данных ИИ.

4. Машинный разум выйдет на массовый рынок, станет постоянным спутником и персональным помощником человека.

5. Рост вычислительных мощностей даст ИИ достаточно возможностей для решения самых сложных задач, вероятны качественные прорывы в прикладных и теоретических науках.

6. Постоянное обучение и работа в разных областях приведет к тому, что каждый достаточно долго функционирующий ИИ будет обретать индивидуальность.

7. На определенной стадии развития компьютерный разум обретет сознание и свободу воли.

Заключение

Несмотря на предложенные Google и Facebook так называемые системы «искусственного интеллекта», полноценная его разработка и существование все еще относится к области фантастики.

В данной работе была сделана попытка всего лишь дать определение искусственному интеллекту путем рассмотрения основных областей его исследования и применения. Искусственный интеллект это молодая и многообещающая область науки, основная цель

которой – найти эффективный способ понимания и применения интеллектуального решения проблем планирования и навыков общения к широкому кругу практических задач. Несмотря на разнообразие проблем, затрагиваемых исследованиями ИИ, во всех отраслях этой сферы наблюдаются некоторые общие черты [2].

1. Использование компьютеров для доказательства теорем, распознавания образов, обучения и других форм рассуждений.
2. Внимание к проблемам, не поддающимся алгоритмическим решениям. Отсюда – эвристический поиск как основа методики решения задач в ИИ.
3. Принятие решений на основе неточной, недостаточной или плохо определенной информации и применение формализмов представлений, помогающих программисту справляться с этими недостатками.
4. Выделение значительных качественных характеристик ситуации.
5. Попытка решить вопросы семантического смысла, равно как и синтаксической формы.
6. Ответы, которые нельзя отнести к точным или оптимальным, но которые в каком-то смысле «достаточно хороши». Это результат применения эвристических методов в ситуациях, когда получение оптимальных или точных ответов слишком трудоемко или невозможно вовсе.
7. Использование большого количества специфичных знаний в принятии решений – основа экспертных систем.
8. Использование знаний метауровня для более совершенного управления стратегиями принятия решений. Хотя это очень сложная проблема, затронута лишь несколькими современными системами, она постепенно становится важной областью исследований.

Литература

1. Свободная энциклопедия «Википедия» [Электронный ресурс] / Интернет-ресурс. – Режим доступа: ru.wikipedia.org.
2. Люггер, Дж. Ф. Искусственный интеллект. Стратегии и методы решения сложных проблем / Дж. Ф. Люггер. – Москва : Вильямс, 2003. – 864 с.
3. Портал искусственного интеллекта [Электронный ресурс] / Интернет-ресурс. – Режим доступа: neuronus.com/history/4-istoriya-vozniknoveniya-ikustvennogo-intellekta.html.
4. Turing, A.M. Computing machinery and intelligence // Mind. – Oxford: Oxford University Press, 1950. – No. 59. – P. 433 - 460.
5. Информационный портал Stas'M Corp. [Электронный ресурс] / Интернет-ресурс. – Режим доступа: stascorp.com/publ/4-1-0-31.
6. Информационное издание Vesti.ru [Электронный ресурс] / Интернет-ресурс. – Режим доступа: hitech.vesti.ru/article/685445.
7. Консорциум MNS.ORG [Электронный ресурс] / Интернет-ресурс. – Режим доступа: www.nmc.org.
8. СКБ Контур [Электронный ресурс] / Интернет-ресурс. – Режим доступа: kontur.ru/articles/4779.

Лапшина Е. В., Ефименко К. Н. Перспективы и сложности развития искусственного интеллекта. *Рассматривается история развития искусственного интеллекта, проблемы его разработки, современные тенденции и направления в развитии, основные области практического применения.*

Ключевые слова: *искусственный интеллект, история развития, проблемы разработки, практическое применение.*

Lapshina K. V., Efimenko K. N. Prospects and difficulties the development of Artificial Intelligence. *The article considers the history of artificial intelligence and the problems of its development. Within the framework of the article, two of the most fundamental problems of AI developers are analyzed. The text gives valuable information on the origins of AI from the middle ages to the present day. It is described current trends and trends in the development of AI. Much attention is given to the description of its main areas of practical application. It is specially noted an active application of achievements of AI-developments in the sphere of military armament and strategy. In this connection, it is raised the question of the danger that AI may pose to humanity. The article is given a list of modern leading world scientific centers that deal with practical research in the field of AI. Based on the analysis of this area, it is singled out the common features of all branches. Attempts are made to formulate a conclusion about the perspectives of the existence and development of AI as a constant companion and personal assistant of human.*

Keywords*: artificial intelligence, history of development, development problems, practical application.*

Статья поступила в редакцию 18 мая 2018 г.
Рекомендована к публикации профессором Шелеповым В. Ю.

УДК 004.5

Применение контроллера Arduino Mega 2560 для разработки геймифицированного теста функциональных состояний учащихся

Д. Д. Зайка, С. В. Плотникова
Государственное бюджетное нетиповое общеобразовательное учреждение
«Республиканский лицей-интернат «Эрудит» – центр для одаренных детей»
Министерства образования и науки Донецкой Народной Республики
dianissimka@gmail.com

Зайка Д. Д., Плотникова С. В., Применение контроллера Arduino Mega 2560 для разработки геймифицированного теста функциональных состояний учащихся. *Робототехника сейчас используется во всех областях человеческой жизни: как в науке, обучении, производстве и медицине, так и в развлекательных проектах. Специфические особенности лицея значительно интенсифицируют учебно-воспитательный процесс, но при этом являются стрессом и могут приводить к снижению успешности обучения. Для оптимизации обучения важно изучение функциональных состояний учащихся, что облегчается при исследованиях в виде игры (геймификации). Для изучения функциональных состояний создан инструмент игра «Настольный футбол» на платформе ArduinoMega 2560, который позволяет упростить и улучшить изучение функциональных состояний учащихся лицея.*

Ключевые слова: робототехника, геймификация, Arduino Mega, футбол.

Введение

В последнее время во всем мире наблюдается резкий рост исследований и проектов в области робототехники. Робототехника сейчас используется во всех областях человеческой жизни: как в серьезных научных проектах, обучении, производстве и медицине, так и в развлекательных целях.

Специфические особенности лицея (профилизация обучения, поиск и целенаправленный конкурсный отбор наиболее способных учащихся, интенсификация обучения, работа в научных кружках, изменения в привычном учебном процессе для учеников, особенности интернатного обучения и др.) значительно интенсифицируют учебно-воспитательный процесс в целом, но при этом являются стрессом и фактором риска здоровья учащихся. Эти факторы могут приводить к преждевременному утомлению, снижению работоспособности, ухудшению состояния здоровья, а, следовательно, и успешности обучения в целом [1, 2].

При этом традиционные методики изучения функциональных состояний не всегда принимаются испытуемыми, в отличии от исследования в виде игры (геймификации).

Точная оценка функционального состояния человека до сих пор является актуальной задачей. Например, анализ данных психофизиологических состояний учеников старших классов необходим для совершенствования методик обучения. Правильный режим труда и отдыха позволяет эффективно и оптимально использовать рабочее время, тогда как без оценки функциональных состояний разработка такого режима представляет значительные затруднения [1, 2].

Цель статьи: изучить возможности современных контроллеров, создать прототип прибора для тестирования некоторых психофизиологических параметров учеников лицея с использованием контроллера и с помощью этого создать автомат.

В соответствии с целью ставятся и решаются следующие задачи:

- изучить возможности современных микроконтроллеров и контроллеров и выбрать платформу для создания прибора.
- разработать аппаратную часть игры «Футбол» с помощью подходящего контроллера.
- разработать программное обеспечение для программно-аппаратного комплекса для игры «человек против человека».
- провести необходимое количество игр среди учеников лицея в разные дни недели в разное время с фиксацией параметров игры. Обработать и изучить данные, полученные после решения предыдущей задачи, определить особенности параметров функциональных состояний (время реакции, стратегии игры и т.д.) в разных группах учащихся в зависимости от пола и возраста; в разное время (после

выходных, в середине и в конце учебной недели, до занятий и после занятий).

– на основе полученных данных доработать программное обеспечение для полноценного решения поставленных задач.

Материалы и методы

В качестве предварительного прототипа для выполнения задачи по созданию геймифицированного инструмента для тестирования функциональных состояний учащихся лицея было решено использовать разработанное в СССР устройство «Электроника ИМ-37» Настольная электронная игра «Футбол: Кубок чемпионов».

Оригинальная версия игры построена на микроконтроллере КР1814ВЕ8 и состоит из светодиодного игрового поля (28 красных светодиодов); поля текущего счета с одноразрядной светодиодной индикацией; 4-х кнопок для каждого игрока, три клавиши – направление удара, одна — перехват мяча; переключателей, расположенных на торцевой части, используемых для включения, а также установки типа и скорости игры.

В оригинальную конструкцию было решено внести несколько изменений – использовать светодиоды 2-х цветов (12 красных и 12 зеленых) для индикации игроков разных команд, а также 4 трехцветных светодиода с общим катодом для индикации угловых и выхода мяча за поле, добавить кнопку для передачи мяча назад, заменить одноразрядные индикаторы счета на многофункциональный символьный жидкокристаллический индикатор (ЖКИ) 16 на 2 символа (LCD1602 I2C).

После изучения возможностей современных микроконтроллеров и контроллеров для дальнейшей работы были выбраны контроллеры семейства Arduino.

Изучены характеристики контроллеров семейства Arduino [3 – 14]. Данное семейство контроллеров отличают полностью открытые аппаратные и программные части, высокая доступность, низкая цена. Программное обеспечение (ПО) можно создавать при помощи официальной свободной интегрированной среды разработки (Arduino IDE) с использованием простого диалекта C++ (Wiring), а также при помощи множества других сред разработки и языков, включая диалект SCRATCH для детей. Большинство контроллеров оснащены широко распространенным интерфейсом USB и загрузчиком, позволяющими обойтись без программаторов. Все вышеперечисленное сделало данное семейство очень распространенным и популярным, что в свою очередь привлекло множество энтузиастов к работе над платформой и наработке множества готовых свободных библиотек ПО, электронных модулей и готовых проектов. Таким образом, семейство Arduino позволяет сосредоточиться на разработке прототипов, а не на изучении устройства и принципов функционирования отдельных элементов.

Наличие готовых модулей, а также плат расширения, монтируемых прямо на контроллер (в терминологии сообщества Arduino шилдов (shield – щиток)), и библиотек программ позволяет непрофессионалам в электронике быстро и просто создавать готовые работающие устройства для решения своих задач. Варианты использования Arduino ограничены только возможностями микроконтроллера и имеющегося варианта платы.

Очевидно, что только для прямого подключения всех светодиодов без сдвиговых регистров к контроллеру необходимо задействовать 36 цифровых выводов, поэтому в качестве платформы для создания устройства был выбран контроллер Arduino Mega 2560, поскольку он имеет необходимое оснащение.

Платформа Arduino Mega 2560 построена на микроконтроллере ATmega2560. Плата имеет 54 цифровых порта ввода/вывода (14 из которых могут использоваться как выводы с широтно-импульсной модуляцией (ШИМ), 16 аналоговых вводов, 4 последовательных порта UART TTL, I2C, SPI, кварцевый генератор 16 МГц, USB-UART преобразователь, разъем питания, разъем ICSP и кнопку перезагрузки.

В микроконтроллерах ATmega2560, используемых на платформах Arduino Mega, существует три вида памяти: флеш-память – используется для хранения программ (в терминологии сообщества Arduino скетчей (sketch – эскиз)); ОЗУ (статическая оперативная память) – служит для хранения и работы переменных; EEPROM (энергонезависимая память) – применяется для хранения постоянной информации. Флеш-память и EEPROM являются энергонезависимыми видами памяти (данные сохраняются при отключении питания). ОЗУ является энергозависимой памятью.

Контроллер обладает достаточным быстродействием для решения поставленных задач, поскольку 1 такт работы микроконтроллера выполняется за 1 с / 16000000Гц * 1000000мкс = 0,0625мкс, то даже операции, выполняемые за несколько сотен тактов будут исполнятся быстрее 1 мс, что значительно меньше погрешности для большинства необходимых измерений, так, например, среднее время реакции на ожог у человека порядка 150-200мс.

Для создания устройства дополнительно были использованы: модуль SD карты с SD картой для записи журналов тестирования и хранения звуковых файлов, плата расширения

PCB для Arduino Mega2650, динамик, тумблеры, потенциометры.

ПО для устройства написано на диалекте C++ для Arduino с использованием официальной IDE. Для написания ПО проекта использовались открытые библиотеки: Wire и LiquidCrystal_I2C для управления ЖКИ, MsTimer2 для работы с прерываниями по таймеру, SD и SPI для работы с SD картой, TMRpcm для воспроизведения звуковых файлов.

Разработка аппаратной части устройства производилась с использованием ПО Fritzing.

Соединения компонентов между собой в устройстве выполнены навесным монтажом.

Разработка игры «Футбол»

В процессе работы над проектом активно использовалась система версионирования Git, материалы проекта расположены на сайте Gitlab [14].

Аппаратная часть устройства очень проста – все исполнительные устройства кроме трехцветных светодиодов подключены непосредственно к цифровым портам вывода контроллера (светодиоды к портам 22-45, динамик – 46 и т. д.), трехцветные светодиоды подключены к аналоговым портам 2-13 для возможного использования ШИМ регулировки яркости каждого цвета. Датчики подключены к цифровым и аналоговым портам ввода (кнопки к портам A0-A9, переключатели и переменные резисторы 47-49, A15). ЖКИ подключен к портам шины I2C (20, 21), а модуль SD карты к портам SPI (50-53).

Для всех светодиодов подключение осуществляется через токоограничивающий резистор на 220 ом. Динамик подключен через усилитель на 1 транзисторе.

Для программирования событий используются режимы игры с соответствующими числовыми кодами: GAME_START 0, GAME_PERFORMED 1, GAME_SIDE_OUT 2, GAME_END_OUT 3, GAME_OFFSIDE 4, GAME_HALFEND 5, GAME_STOP 6, GAME_GOAL 9, для жеребьевки, непосредственно игры, выхода мяча за боковую линию, а также за линию ворот, превышения времени удержания мяча одним игроком, окончания первого тайма, окончания игры и взятия ворот соответственно.

Для каждого события написан обработчик в виде функции, которая выполняется из тела функции loop(), при соответствии режима игры определенному значению.

Игровое поле разделено координатной сеткой на прямоугольные области 12x5. Это x и y координаты мяча, при попадании мяча в соответствующую область загорается светодиод, расположенный в этой области.

На игровом поле расположены по 12 светодиодов красного и зеленого цветов, по 11 соответствуют игрокам, и по 1 для индикации взятия ворот. В программе для работы со светодиодами создан трехмерный массив 12x5x2, где первые 2 индекса указывают на координаты светодиода, а 3-й на номер порта и цвет (для трехцветных светодиодов вместо номера порта индекс по которому расчитывается номер порта). Пустые области обозначаются числом -1 (минус единица), цвета 1 (единица) — зеленый, -1 (минус единица) — красный, пустая область и трехцветные светодиоды — 0 (ноль):

Каждый игрок управляет игрой при помощи 4-х кнопок для перемещения мяча и 1-й кнопки для перехвата мяча.

Для работы с кнопками в программе создан класс, обрабатывающий дребезг и описывающий необходимые свойства и методы кнопок. Для считывания состояния кнопок используется прерывание по таймеру с интервалом в 15мс.

Для перемещения мяча при помощи комбинации кнопок используется суммирование условных баллов за каждую кнопку — так нажатие кнопки вперед оценивается в 3 балла, назад в -3, влево в -1 и вправо в 1 балл, суммы баллов рассматриваются как направления для перемещения мяча соответственно схеме:

```
// directions
// 2  3  4
// -1  0  1
// -4  -3  -2
```

Игра начинается с жеребьевки, когда после звукового сигнала и соответствующего сообщения на ЖКИ игрокам нужно как можно быстрее нажать на кнопку перехвата мяча. Выигрывает игрок, который нажал на кнопку раньше после звукового сигнала, и не допустил фальстарт.

Игра состоит из 2x таймов по 3 минуты. После жеребьевки мяч перемещается к игроку команды выигравшей жеребьевку в центре поля, в начале 2-го тайма мяч перемещается к игроку команды проигравшей жеребьевку в центре поля. Удержание мяча игроком без перемещения более чем на 10с приводит к обработке GAME_OFFSIDE и мяч перемещается к игроку в центре поля. После выхода мяча за боковую линию мяч возвращается к ближайшему игроку противоположной команды. После выхода мяча за линию ворот мяч возвращается к игроку противоположной команды для выполнения углового удара или к вратарю для удара от ворот. Для рандомизации в игре при каждом вызове функции loop() выбрасывается условная семигранная кость с гранями от -3 до 3. При перемещении мяча по полю через область с игроком мяч может быть перехвачен в течении заданного времени перехвата кнопкой перехвата, это событие вероятностное, оно определяется

суммой заданной вероятности перехвата и текущей выпавшей гранью кости. При перемещении мяча в координаты ворот противоположной команде добавляется 1 балл (очко) к сумме балов (очков) с вероятностью, определяемой суммой заданной вероятности поражения ворот (гола) и текущей выпавшей гранью кости, если ворота не поражены, игра перейдет к режиму выхода за линию ворот.

Победа засчитывается стороне, набравшей больше очков, иначе объявляется ничья.

Все события, происходящие в течении игры записываются в файл журнала со случайным названием, уникальным для каждой игры, для последующей обработки и сравнения. Журнал позволяет далее проанализировать время реакции игроков на события игры, стратегии игры, качество принимаемых участниками игры решений.

Выводы

Выбранная платформа позволяет качественно решить все поставленные в работе задачи.

Аппаратная часть проекта создана на платформе Arduino Mega 2560. Разработанное ПО для игры «человек против человека» позволяет проводить геймифицированное тестирование функционального состояния учащихся лицея для получения данных, используемых в дальнейшей работе над оптимизацией обучения. А затем после сбора данных, создания автомата «человек против компьютера».

В дальнейшем после проведения необходимого количества игр, полученные результаты будут использованы для создания автоматического режима игры «компьютер против человека», что позволит проводить тестирование с одним испытуемым.

Литература

1. Шмелёв А., Лисица И., Компьютерное тестирование и геймификация: перспективы мониторинга функционального состояния работников в эпоху компьютеризации психодиагностики [Электронный ресурс] – 2016 – Режим доступа: https://cyberleninka.ru/article/n/kompyuternoe-testirovanie-i-geymifikatsiya-perspektivy-monitoringa-funktsionalnogo-sostoyaniya-rabotnikov-v-epohu-kompyuterizatsii – Загл. с экрана.

2. Алексеева Э.А, Шантанова Л.Н., Петунова А.Н. , Иванова И.К. Оценка функционального состояния организма студентов в период экзаменационного стресса [Электронный ресурс] – 2010 – Режим доступа: https://cyberleninka.ru/article/n/otsenka-funktsionalnogo-sostoyaniya-organizma-studentov-v-period-ekzamenatsionnogo-stressa – Загл. с экрана.

3. Омельченко Е.Я., Танич В.О., Маклаков А.С., Карякина Е.А. Краткий обзор и перспективы применения микропроцессорной платформы arduino [Электронный ресурс] – 2013 – Режим доступа:. https://cyberleninka.ru/article/n/kratkiy-obzor-i-perspektivy-primeneniya-mikroprotsessornoy-platformy-arduino – Загл. с экрана.

4. Официальный практикум Arduino // [Электронный ресурс]. – 2017 – Режим доступа: https://www.arduino.cc/en/Tutorial – Загл. с экрана.

5. Петин В.А. Проекты с использованием контроллера Arduino. СПб. : БХВ-Петербург, 2015. – 448 с.

6. Плат Ч. Электроника для начинающих //Пер. с англ. – 2-е изд. – СПб.: БХВ – Петербург, 2017. – 416 с

7. Официальный репозиторий и документация библиотеки Arduino MsTimer2 // [Электронный ресурс]. – 2016 – Режим доступа: https://github.com/PaulStoffregen/MsTimer2 – Загл. с экрана.

8. Официальный репозиторий и документация библиотеки ArduinoLiquidCrystal-I2C-library // [Электронный ресурс]. – 2017 – Режим доступа: https://github.com/fdebrabander/Arduino-LiquidCrystal-I2C-library – Загл. с экрана.

9. Официальный репозиторий и документация библиотеки Arduino SD Library for Arduino // [Электронный ресурс]. – 2017 – Режим доступа: https://github.com/arduino-libraries/SD – Загл. с экрана.

10. Официальный репозиторий и документация библиотеки Arduino TMRpcm Arduino library for asynchronous playback of PCM/WAV files direct from SD card [Электронный ресурс]. – 2017 – Режим доступа: https://github.com/TMRh20/TMRpcm – Загл. с экрана.

11. Официальный справочник Arduino // [Электронный ресурс]. – 2017 – Режим доступа: https://www.arduino.cc/en/Reference/HomePage – Загл. с экрана.

12. Русскоязычный wiki справочник ардуино [Электронный ресурс]. – 2017 – Режим доступа: http://wikihandbk.com/wiki/Arduino – Загл. с экрана.

13. Урок 10. Прерывание по таймеру в Ардуино. Библиотека MsTimer2. Параллельные процессы [Электронный ресурс]. – 2016 – Режим доступа: http://mypractic.ru/urok-10-preryvanie-po-tajmeru-v-arduino-biblioteka-mstimer2-parallelnye-processy.html – Загл. с экрана.

14. Arduino-soccer [Электронный ресурс] – 2017 – Режим доступа: https://github.com/ventricola/arduino-soccer – Загл. с экрана.

Зайка Д. Д., Плотникова С. В., Применение контроллера Arduino Mega 2560 для разработки геймифицированного теста функциональных состояний учащихся. *Робототехника сейчас используется во всех областях человеческой жизни: как в науке, обучении, производстве и медицине, так и в развлекательных проектах. Специфические особенности лицея значительно интенсифицируют учебно-воспитательный процесс, но при этом являются стрессом и могут приводить к снижению успешности обучения. Для оптимизации обучения важно изучение функциональных состояний учащихся, что облегчается при исследованиях в виде игры (геймификации). Для изучения функциональных состояний создан инструмент игра «Настольный футбол» на платформе* ArduinoMega *2560, котрый позволяет упростить и улучшить изучение функциональных состояний учащихся лицея.*

Ключевые слова: робототехника, геймификация, Arduino Mega, футбол.

Zajaka D. D., Plotnikova S. V., Application of the Arduino Mega 2560 comptroller for developent of gameficication test of the functional states studying. *Robot techique is now used in all spheres of human life: how in science, teaching, production and medicine, so in entertaining projects. The specific features of lyceum considerably intensify an study process, but here are stress and can result in the decline of success of teaching. For optimization of teaching the study of the functional states studying is important, that is facilitated at researches as the game (gameficication). For the study of the functional states an instrument is created the game «Table football» on the ArduinoMega 2560 platform, allows to simplify and improve the study of the functional states of studying lyceum.*

Keywords: r*obot techique* , *gameficication*, Arduino Mega, football.

Статья поступила в редакцию 18 мая 2018 г.
Рекомендована к публикации профессором Миненко А. С.

УДК 004.056.55

Разработка алгоритма хеширования информации на основе метода наименьших квадратов

А. А. Кобец, Н. В. Марковская
МОУ «Специализированная физико-математическая школа №17»
kobetc.rey8@gmail.com, marknata@mail.ru

Кобец А. А., Марковская Н. В. Разработка алгоритма хеширования информации на основе метода наименьших квадратов. *В статье описывается необходимость разработки новых принципов хеширования, а также формулируются требования к функциям, реализующим получение дайджестов сообщений. Выдвигается и обосновывается гипотеза о возможности использования метода наименьших квадратов в качестве метода получения дайджеста сообщений. Приводится разработанный алгоритм, построенный на базе данной гипотезы.*

Ключевые слова*: криптография, хеширование, дайджест, МНК.*

Постановка проблемы

В человеческом обществе все более актуальной становится проблема опасности перехвата конфиденциальной информации при работе с ней. Современная криптография для обеспечения защиты данных использует наборы преобразований, называемых криптографическими примитивами.

В частности, для обеспечения безопасного хранения и сравнения информации, используются дайджест-функции. Однако, возникает проблема кодировки, которая базируется на сравнительной простоте большого числа используемых дайджест-функций.

Стремительный рост производительности вычислительной техники позволяет говорить о реальных временных промежутках при применении brute-force атак (от 30 минут до 45 часов). К тому же продолжительное изучение криптоаналитиками данных алгоритмов, позволяет находить коллизии за минуты.

Таким образом, для решения данной проблемы необходима разработка совершенно нового способа хеширования, основанного на ранее не использовавшихся принципах.

Цель

Целью данной работы является создание оптимального алгоритма хеширования, основанного на методе наименьших квадратов.

Анализ существующих разработок

На данный момент существует большое количество алгоритмов хеширования. Многие из них реализуют, так называемую, блочную структуру. Наиболее показательными примерами таких алгоритмов являются дайджест-функции MD5 и SHA-1.

MD5 – это 128-битный алгоритм хеширования. Данный алгоритм был разработан Рональдом Л. Ривестом из Массачусетского технологического института как более надёжная версия алгоритма MD4. Впервые был описан в RFC – 1321 [1].

Основным достоинством алгоритма MD5 является наличие, так называемого, «лавинного эффекта». Это означает, что незначительное изменение в открытом тексте, передаваемое данному алгоритму, вызовет кардинальное изменение в результирующем хеше.

Однако, ещё в 2006 году чешский исследователь Властимил Клима опубликовал алгоритм, в последствии названный «туннелированние» [2]. Данный алгоритм позволял находить коллизии MD5 на домашнем компьютере за полминуты. В следствие чего, в конце 2008 года MD5 был признан небезопасным, и организация US-CERT призвала прекратить использовать MD5 в любых целях.

Не смотря на это, многие разработчики активно применяют его до сих пор.

SHA-1, описанный в RFC 3174 [3], – как и MD5, является усовершенствованной версией алгоритма MD4. Важным отличием SHA-1 от MD5 является то, что на выходе получаемая последовательность имеет длину 160 бит. Как и MD5, SHA-1 присущ лавинный эффект, более того, данный алгоритм гораздо более устойчив к поиску коллизий, нежели описанный выше.

Тем не менее, несмотря на то, что SHA-1 несколько более сложен по своей структуре, нежели MD5, подбор пароля при помощи brute-force – атаки, по заданному дайджесту SHA-1 не является проблемой. Семизначный пароль, в котором есть символы латинского алфавита, а также цифры 0-9 и спецсимволы подбирается примерно за 31 час[4].

Определение требований к надёжному алгоритму хеширования

В криптографии существует ряд требований к хеш-функциям:

1. Необратимость – для дайджеста, построенного заданной хеш-функцией должно быть вычислительно невозможно найти прообраз.
2. Стойкость к коллизиям первого рода – для заданного сообщения должно быть вычислительно невозможно подобрать такой аналог, чтобы в обоих случаях функция вернула одинаковый результат.
3. Стойкость к коллизиям второго рода - должно быть вычислительно невозможно найти пару сообщений, для которых заданная хеш-функция вернёт одинаковый результат.

Так же стоит отметить, что подавляющее большинство современных хеш-функций реализует «лавинный эффект» - свойство дайджеста значительно изменяться даже при незначительных отличиях исходных последовательностей.

Разработка алгоритма

Метод Наименьших Квадратов (МНК англ. ***Ordinary Least Squares, OLS***) – это метод регрессионного анализа, позволяющий сгладить результаты наблюдений, содержащих случайные ошибки.

Именно на нём построен основной принцип работы алгоритма.

Выбор данного метода обоснован следующими его свойствами:

1. Для трёх точек, не принадлежащих одной прямой, шанс вхождения одной отдельно взятой точки во множество решений аппроксимирующей линейной функции, сравнительно мал, а также невозможно сказать в какую сторону происходит отклонение. По этим причинам, истинное положение точки не может быть воспроизведено аналитически.
2. Изменение положения любой из искомых точек отражается на конечном результате в достаточно большой степени, чтобы вызвать «лавинный эффект».

Для реализации алгоритма был выбран язык программирования Java, так как его среда исполнения поддерживается большинством современных устройств, а так же в состав его стандартной библиотеки входят классы, реализующие возможность использования вещественных чисел с неограниченной разрядностью, что весьма важно для увеличения эффективности результата.

Вычисление дайджеста сообщения происходит в три условных этапа:

1. Вычисление первичной числовой комбинации.
2. Вычисление вторичной числовой комбинации.
3. Слияние распределение комбинаций по массиву байт требуемой длины.

Вспомогательные функции

В ходе вычисления дайджест последовательности, алгоритм неоднократно обращается к следующим вспомогательным функциям:

1. **pseudoRandom(seed, mix)** - Данная функция предназначена для генерации псевдослучайных чисел, вычисляемых на основе двух аргументов по следующему алгоритму:
   1. Инициализируется переменная $a = \sin(\cos(seed)) * 100$;
   2. Выполняется присваивание $a = a \cdot sin((int)(a * 100))$. В данном случае (int) означает приведение к целочисленному типу с отбрасыванием всех разрядов меньше единицы.
   3. Значение a переводится из радианов в градусы.
   4. Выполняется присваивание $a = a \cdot \sin(mix)$;
   5. Значение a приводится к целочисленному типу с отбрасыванием всех разрядов меньше единицы
   6. Значению a присваивается сумма первых двух и последних двух разрядов.
   7. На выходе данная функция возвращает **|*a*|**.

   При условии, что параметры данной функции лежат в интервале [0;65536], её результат будет лежать в промежутке [0-146].

2. **arrayShuffle(array, rndSeed);**

   Данная функция предназначена для перестановки элементов массива на основе вышеописанного ГПСЧ. Работает по следующему алгоритму:
   1. Для каждого i-го элемента массива:
   2. Вычисляется число j, такое, что:

$$j = (int)\left(\left(\frac{pseudoRandom(rndSeed,i)}{144}\right) * i\right) \quad (1)$$

   Исходя из формулы, $j \in [0; i]$;
   3. Меняются элементы массива с номерами i, j местами;
   4. По завершении цикла, функция возвращает преобразованный массив.

3. arrayXOR(bytes, bytes1)

Данная функция выполняет сложение по модулю 2 всех элементов принимаемых массивов, а так же – корректирует их длины. Данная функция реализует следующий алгоритм:

1) Если длины массивов совпадают, действия 2-3 пропускаются.
2) Избыточные элементы поочерёдно суммируются по модулю два со всеми элементами массива, имеющего лишнюю длину.
3) Выполняется уравнивание длин массивов.
4) Для *i*-го элемента массива *bytes* выполняется действие:

$$bytes1[i] = bytes[i] \oplus bytes1[i];$$

5) Результат данной функции – массив *bytes1*.

На вход данного алгоритма поступает два значения:

1. *mdLenBytes* – число байт, ожидаемое пользователем, должно входить в натуральные числа.
2. *sequence* – входная последовательность байт.

Входное сообщение разбивается на массив *numbers*, хранящий в себе числовое представление символов исходной строки. Дальнейшие операции производятся уже на нём.

3. В данный массив дописывается число, зависящее исключительно от дины массива и вычисляемого по формуле:

$$len = preLength \oplus pseudoRandom(preLength, preLength);$$

где *preLen* – длина массива до включения в него искомого числа.

4. Длина исходного массива увеличивается до ближайшего числа кратного 9. При этом новые элементы заполняются элементами из старого (по «кольцевой схеме». Например, при исходном массиве = [5, 4, 3], новый массив выглядит следующим образом: [5, 4, 3, 5, 4, 3, 5, 4, 3]).
5. Затем выполняется цикл, в котором все значения исходного массива заменяются по следующему принципу:

$$numbers[i] = 1 + \left(\frac{pseudoRandom(numbers[i],i)}{144}\right) \cdot 65536; \quad (2)$$

6. Первый этап – получение первичной хеш-последовательности:

Из созданного массива вычисляется трёхмерная матрица *matrix*, размером [N][3][3]. Данная матрица при дальнейших операциях интерпретируется как N избыточных систем линейных уравнений вида:

$$\begin{cases} matrix[i][0][0] \cdot x + matrix[i][0][1] \cdot y = matrix[i][0][2]; \\ matrix[i][1][0] \cdot x + matrix[i][1][1] \cdot y = matrix[i][1][2]; \\ matrix[i][2][0] \cdot x + matrix[i][2][1] \cdot y = matrix[i][2][2]; \end{cases} \quad (3)$$

где i – номер данной системы.

Для простоты обозначения, введены специальные обозначения:

$$A_{i_j} = matrix[i][j][0]; B_{i_j} = matrix[i][j][1]; \quad (4)$$
$$C_{i_j} = matrix[i][j][2];$$

С учётом введённых обозначений, система 3 будет выглядеть следующим образом:

$$\begin{cases} A_{i_1} \cdot x + B_{i_1} \cdot y = C_{i_1}; \\ A_{i_2} \cdot x + B_{i_2} \cdot y = C_{i_2}; \\ A_{i_3} \cdot x + B_{i_3} \cdot y = C_{i_3}; \end{cases} \quad (5)$$

Данная избыточная система легко решается при помощи метода наименьших квадратов. После всех преобразований, выводится формула, являющаяся явным представлением пары чисел (X, Y):

$$\begin{cases} X = \frac{\sum_{j=0}^{n} A_{i\,j}^2 \cdot \sum_{j=0}^{n} A_{i\,j} C_{i\,j} - \sum_{j=0}^{n} A_{i\,j} B_{i\,j} \cdot \sum_{j=0}^{n} B_{i\,j} C_{i\,j}}{\sum_{j=0}^{n} B_{i\,j}^2 \cdot \sum_{j=0}^{n} A_{i\,j}^2 - \left(\sum_{i=0}^{n} A_{i\,j} B_{i\,j}\right)^2}; \\ Y = \frac{\sum_{j=0}^{n} A_{i\,j} C_{i\,j} - \sum_{j=0}^{n} A_{i\,j}^2 \cdot X}{\sum_{i=0}^{n} A_{i\,j} B_{i\,j}}; \end{cases} \quad (6)$$

где n – это количество рассматриваемых уравнений – 1 (в данном случае: 3-1= 2).

Результаты вычислений записываются в двумерную матрицу results.

Первичная хеш-последовательность представляет собой множество, состоящее из двух чисел и являющееся произведением полученных результатов.

Очень важно сохранить максимальную точность данного числа, т. к. от этого будет зависеть насколько сложен будет дайджест в результате работы алгоритма поэтому рекомендуется использовать типы данных, позволяющие работать с неограниченным количеством символов после запятой, например BigDecimal в языке Java.

Второй этап – получение вторичной хеш-последовательности.

Данный этап, как и предыдущий основывается на методе наименьших квадратов. Однако, в данном случае, вместо использования его в качестве метода решения избыточных систем, здесь реализуется ещё одно применение данного метода. При получении вторичного хеша, данный метод используется для получения коэффициентов линейного уравнения, наиболее точно описывающего последовательность точек:

$$\left(i;\ pseudoRandom(sequence[i], i)\right) \quad (7)$$

где i – номер позиции символа в передаваемой последовательности.

Т. к. первое число является координатой *i*-ой точки на оси абсцисс, обозначим его как X_i, а второе, соответственно Y_i.

Явный вид параметров линейного уравнения:

$$\begin{cases} A = \frac{\sum_{i=0}^{n-1} X_i \cdot \sum_{i=0}^{n-1} Y_i - n \cdot \sum_{i=0}^{n-1} X_i Y_i}{(\sum_{i=0}^{n-1} x_i)^2 - n * \sum_{i=0}^{n-1} X_i Y_i} \\ B = \frac{1}{n} \cdot (\sum_{i=0}^{n-1} Y_i - A \cdot \sum_{i=0}^{n-1} x_i \end{cases} \quad (8)$$

Также следует указать, для достижения наилучшего эффекта, требуется использовать то же количество символов после запятой, что и у первичной хеш-последовательности.

Множество {A, B} является вторичной хеш-последовательностью.

1. Далее все составляющие элементы, составляющие первичную и вторичную хеш-последовательности переводятся в массивы байт.
2. Объявляется массив fusionArray, который, в последствии, будет хранить объединённые значения первичного и вторичного хеша.
3. Выполняются следующие действия:

$fusionArray[0] = arrayXOR(primaryHash[0], secondaryHash[0]);$
$fusionArray[1] = arrayXOR(primaryHash[1], secondaryHash[1]);$

где primaryHash[0], primaryHash[1], secondaryHash[0], secondaryHash[1] – первые и вторые цифры первичной и вторичной хеш последовательности соответственно.

4. Создаётся переменная *hash*, в которую записывается следующее значение:

$hash = arrayXOR(fusionArray[0], fusionArray[1]);$

5. Каждый элемент массива подвергается изменению при помощи формулы:

$hash[i] = hash[i] \oplus (pseudoRandom(i, hash[i]) \oplus i;$

где i – номер элемента в массиве.

6. Положение значений в массива *hash* меняется в псевдослучайном порядке:

$hash = arrayShuffle(hash, (slength \oplus hashLength));$

где slength и hashLength длина исходной строки и длина хеша соответственно.

7. Повторение действия 11.
8. Создаётся returnHash изаполняется по следующему алгоритму: для i, не превышающего длины массива элемента массива:

$returnHash[i] = pseudoRandom(i, hash.length \oplus mdLenBytes);$

9. Выполняется слияние сгенерированных и полученных раннее данных.

В цикле с переменной-счётчиком i, не превышающем длину массива hash, проверяется условие. Существует ли i-й элемент в массиве returnHash. Если условие верно, то выполняется простейшее преобразование:

$returnHash[i] = returnHash[i] \oplus hash[i];$

Иначе, выполняется вход в другой цикл, в котором изменяются все элементы массива returnHash номера которых кратны остатку от деления i на размер массива returnHash. Изменение происходит по следующщему примеру:

$returnHash[j] = returnHash[j] \oplus hash[i];$

где j – это номер элемента массива, кратный остатку от деления.

10. Если размер массива hash меньше размера массива returnHash, выполняется преобразование:

$returnHash = arrayShuffle(returnHash, pseudoRandom(hash.length, returnHash.length));$

11. Массив returnHash и является искомым дайджестом.

Выводы

В рамках данного исследования был проведён анализ основных уязвимостей криптографических функций. В качестве альтернативы к уже устаревшим алгоритмам был разработан совершенно новый, основанный на ранее не применявшихся принципах алгоритм хеширования.

Литература

1. RFC 1321 [Электронный ресурс] // IETF Tools - Режим доступа: https://tools.ietf.org/html/rfc1321

2. Tunnels in Hash Functions: MD5 Collisions Within a Minute. Vlastimil Klima Prague, Czech Republic [Электронный ресурс] // Режим доступа: http://cryptography.hyperlink.cz/2006/tunnels.pdf

3. RFC 3174 [Электронный ресурс] // IETF Tools Режим доступа: https://tools.ietf.org/html/rfc3174

4. NIST COMMENTS ON CRYPTANALYTIC ATTACKS ON SHA-1 [Электронный ресурс] // National Institute of Standards and Technology - Режим доступа: http://csrc.nist.gov/groups/ST/hash/statement.html

5. Дринфельд Г.И. Интерполирование и способ наименьших квадратов // Г.И. Дринфельд К.: «Вища школа», 1984. - 103 с.

Кобец А. А., Марковская Н. В. Разработка алгоритма хеширования информации на основе метода наименьших квадратов. *В статье описывается необходимость разработки новых принципов хеширования, а также формулируются требования к функциям, реализующим получение дайджестов сообщений. Выдвигается и обосновывается гипотеза о возможности использования метода наименьших квадратов в качестве метода получения дайджеста сообщений. Приводится разработанный алгоритм, построенный на базе данной гипотезы.*

Ключевые слова*: криптография, хеширование, дайджест, МНК.*

Kobets A. A., Markovskaya N. V. Developing hashing information algorithm based on ordinary least squares method. *The article describes the necessity of developing new principles of hashing and formulates the requirements to the functions that realize getting message digests. A new hypothesis which says that ordinary least squares method is suitable as the method of getting message digests had been put forward and justified. Developed algorithm based on this hypothesis is given.*

Keywords*: cryptography, hashing, digest, OLS.*

Статья поступила в редакцию 24 апреля 2018 г.
Рекомендована к публикации профессором Павлышом В. Н.

УДК 004.49

Современные киберпреступления и основы кибербезопасности

А. В. Гром, К. Н. Ефименко
Донецкий национальный технический университет
grom.anastasiya@inbox.ru, KN_Efimenko@mail.ru

Гром А. В., Ефименко К. Н. Современные киберпреступления и основы кибербезопасности. *Рассмотрены основные виды компьютерных преступлений, вредоносных программ и способы мошенничества в сети Internet, а также даны рекомендации по общим принципам защиты от киберпреступлений.*

Ключевые слова: *компьютерные преступления, вредоносные программы, Internet-мошенничество, безопасность.*

Введение

Ежедневно по всему миру все большее количество компьютеров подвергается вирусной атаке. Так 27 июня 2017г. от атаки компьютерного вируса-шифровальщика Petya.A пострадали десятки компаний в РФ и на Украине. 24 октября 2017г. атаке криптовируса-вымогателя Bad Rabbit (англ. «плохой кролик») подверглись компьютеры в РФ, на Украине, в Турции и Германии. И наконец, 3 ноября этого года вирус WCry – сокращение от английского Wanna Cry (англ. «Хочется плакать») проник в сети МВД, МЧС, РЖД, Сбербанка, «Мегафона» России. За 24 часа заражению подверглись 45 тысяч систем в 74 странах. Именно такие вредоносные программы и их массовое распространение заставляет все чаще задумываться о кибербезопасности.

Актуальность изучения вопроса компьютерных преступлений

Стремительный рост научно-технического прогресса является одним из аспектов, влияющих на значительную трансформацию преступности. Компьютерные технологии используются практически во всех сферах жизнедеятельности человека, начиная от контроля над пассажирской транспортной системой и заканчивая решением вопросов национальной безопасности. Распространение компьютерных сетей привело к всеобщему использованию электронной почты, как наиболее удобному средству связи и обмена информацией. Все большую популярность набирает размещение социальной информации, предназначенной для использования большого количества пользователей, в глобальной сети на специализированных сайтах органов управления, ведомств и министерств.

Данные изменения в распространении информации можно отметить как положительные, упрощающие и модернизирующие жизнь современного общества, аспекты. Но вместе с тем не стоит забывать о том, к каким негативным последствиям это может привести. Разработка большого количества разнопланового программного обеспечения, рост производства и совершенствование вычислительных машин, повсеместное использование компьютерной информации разного рода значимости на просторах Интернета, приводят к совершенствованию «традиционных» видов преступных действий (хищение денежных средств и информации разного назначения, подделка документов и ценных бумаг и т.д.) и способствуют созданию новых разновидностей преступлений (компьютерное мошенничество, несанкционированное использование информации и др.).

Целью данной работы является изучение вопросов компьютерных преступлений, выявление общих и особых характеристик разного рода преступлений, совершающихся с использованием компьютерной техники и выбор наиболее действенных способов защиты от вторжения компьютерных преступников.

Характеристики компьютерных преступлений и вредоносных программ

Изучением проблемы компьютерных преступлений в криминалистической науке занимались многие исследователи, например, Н. П. Яблоков, И. Ф. Герасимов, Г. Г. Зуйков, И. Ф. Пантелеев и др. Обзор научной литературы, судебной и следственной практики позволяет сделать вывод, что на данный момент разработаны только частные методики расследования некоторых видов преступлений данной категории, а конкретно методика раскрытия преступлений в сфере компьютерной информации еще не получила достаточного освещения в юридической литературе. Большинство уголовных дел по компьютерным преступлениям остаются нераскрытыми. К сожалению, при высоком техническом оснащении и тщательной подготовке

преступления, поймать киберпреступника очень сложно. Тем не менее, возможно.

Компьютерные преступления – это предусмотренные уголовным законодательством общественно опасные действия, в которых объектом или средством преступного посягательства является машинная информация. Другими словами, в качестве предмета или орудия такого преступления выступает машинная информация, компьютер, компьютерная система или сеть.

Зарубежный и российский опыт свидетельствует о том, что субъекты компьютерных преступлений различаются как по уровню их профессиональной подготовки, так и по социальному положению. «Компьютерных» преступников можно разделить на несколько групп.

Первая группа – нарушители правил пользования ЭВМ. Они совершают преступления из-за недостаточно хорошего знания техники, желания ознакомиться с интересующей их информацией, похитить какую-либо программу или бесплатно пользоваться услугами ЭВМ.

Ко второй группе относят лиц, отличительной особенностью которых является устойчивое сочетание профессионализма в области компьютерной техники и программирования с элементами своеобразного фанатизма и изобретательности, так называемых «хакеров» или «одержимых программистов». Они воспринимают средства компьютерной техники как своеобразный вызов их творческим и профессиональным знаниям, умениям и навыкам, что служит побуждающим фактором для совершения противоправных действий. Характерной особенностью этой группы является отсутствие у преступников четко выраженных намерений получить материальную выгоду. Практически все действия совершаются ими с целью проявления, подтверждения и доказательства своих способностей.

Третьих иногда называют «информационными путешественниками». Они специализируются на проникновении в чужие компьютеры и сети.

Четвертые – создатели троянских программ и компьютерных вирусов. Впрочем, их уже нельзя назвать хакерами, так как: неформальный «кодекс» хакеров запрещает использование своих знаний во вред пользователям. Эту группу составляют профессиональные «компьютерные» преступники, которые совершают противоправные деяния с ярко выраженными корыстными целями. Эти преступники характеризуются многократностью совершения компьютерных преступлений с обязательным использованием действий, направленных на сокрытие преступлений. Они обычно являются членами хорошо организованных и технически оснащенных первоклассным оборудованием преступных групп и сообществ. Чаще всего, это высококвалифицированные специалисты, имеющие высшее техническое, юридическое или экономическое (финансовое) образование. Их целью является получение стратегически важных данных о противнике в экономической, технической и других областях. На долю этих преступников приходится максимальное число совершенных особо опасных посягательств (до 79 % хищений денежных средств в крупных и особо крупных размерах и различного рода должностных преступлений, совершенных с использованием средств компьютерной техники) [1].

Выделяют пять наиболее распространенных мотивов совершения компьютерных преступлений:

1. Корыстные соображения;
2. Политические цели (шпионаж; преступления, направленные на подрыв финансовой и денежно-кредитной политики правительства, на дезорганизацию валютной системы страны, на подрыв рыночных отношений);
3. Исследовательский интерес (студенты и профессиональные программисты);
4. Хулиганские побуждения и озорство (хакеры);
5. Месть.

Условно компьютерные преступления можно разделить на две категории [2]:

1. Преступления, связанные с вмешательством в работу компьютера;
2. Преступления, использующие компьютер как необходимое техническое средство.

Каждая из них связана с несанкционированным доступом к сетям, серверам, машинным ресурсам. Однако, первая категория включает те преступления, в рамках которых вмешательство в работу компьютеров, направлено на повреждение или уничтожение информации, нарушение нормального их функционирования. Наиболее яркий пример – вирусы. В преступлениях второй категории, компьютер выступает не объектом посягательства, но его средством, а целью является получение и использование информации, в том числе, и для совершения иных преступных деяний. Например, хищений денежных средств с банковских счетов. Необходимо отметить, что во многих случаях одно нарушение может иметь признаки преступлений, относящихся к обеим категориям [3].

Компьютерные преступления можно разделить на несколько видов [4].

1. Несанкционированный доступ к информации, хранящейся в компьютере,

осуществляется, как правило, с использованием чужого имени, изменением физических адресов технических устройств, использованием информации, оставшейся после решения задач, модификацией программного и информационного обеспечения, хищением носителя информации, установкой аппаратуры записи, подключаемой к каналам передачи данных.

2. Создание и распространение вредоносных программ – любого программного обеспечения (ПО), предназначенного для получения несанкционированного доступа к вычислительным ресурсам или к информации, хранимой на ЭВМ, с целью несанкционированного владельцем использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путем копирования, искажения, удаления или подмены информации. Вредоносные программы делятся на обычные вирусы, сетевые черви и троянские программы.

К *обычным вредоносным объектам* относят программы, которые распространяют свои дубликаты на локальном компьютере. Главной целью является запуск определённого программного алгоритма при выполнении пользователем некоторых действий или при последовательности действий. Эти вирусы не используют напрямую ресурсы локальной или глобальной сети для размножения, а выполняют заражение исполняемых файлов, перемещаясь на локальные компьютеры других пользователей. Обычные компьютерные вирусы распространяются посредством переноса информации самим пользователем, будь то съёмный носитель, электронная почта или открытые ресурсы локальной сети.

Сетевые черви являются вредоносными объектами, распространяющие свои копии по глобальной или локальной сети, при этом используются так называемые «дыры» в программах и установленных на компьютерах пользователей ОС. Как правило, червь может проникать сквозь почтовое сообщение, при этом будет иметь вид зараженного файла, или через ICQ сообщение. Существуют «пакетные» или «бесфайловые» черви, распространяющиеся посредством сетевых пакетов, при этом используются обычные сетевые протоколы, которые сразу попадают в память компьютера, где активируются самостоятельно.

К *троянским программам* относят все вредоносные программные элементы, использующие информацию либо ресурсы компьютера для своего хозяина. Как правило, происходит шифрование или стирание данных пользователя, пересылка конфиденциальной информации пользователя, воровство паролей доступа к сетевым ресурсам, использование ресурсов компьютера для рассылки спама или атак серверов. Обычно троянские программы не способны нарушить работу зараженного компьютера, они ведут себя достаточно тихо, без особых проявлений.

3. Компьютерный шпионаж или компьютерное пиратство.

Компьютерный шпионаж или кибершпионаж – это методы получения секретной конфиденциальной информации без предварительного разрешения владельцев данной информации (личной, служебной или засекреченной): частных лиц, конкурентов, правительства либо врагов. Такой вид слежения за компьютерами предполагает использование неких методов доступа к секретной, конфиденциальной информации либо контроля компьютерных систем, целых сетей для получения стратегических преимуществ применимых к психологической, политической и физической деятельности, в частности диверсий. В последнее время кибершпионаж все чаще применяется для анализа общественной активности на сайтах соцсетей.

Под *компьютерным пиратством* обычно понимается несанкционированное правообладателем копирование, использование и распространение программного обеспечения. Компьютерное пиратство может принимать различные формы, однако можно выделить несколько наиболее распространенных его разновидностей:

– интернет-пиратство – это распространение нелегальных копий программных продуктов с использованием Интернет. Данная разновидность пиратства выделена специально для того, чтобы подчеркнуть ту большую роль, которую играет сегодня Интернет для незаконного копирования и распространения поддельного и иного незаконно распространяемого программного обеспечения. В понятие Интернет-пиратства входит, в частности, использование глобальной сети для рекламы и публикации предложений о продаже, приобретении или распространении пиратских копий программных продуктов. Сюда же относится публикация в сети Интернет серийных номеров коммерческого ПО.

– нелегальное тиражирование – это широкомасштабное изготовление подделок (ПО и упаковки) и распространение их в каналах продаж под видом легальных продуктов. Для изготовления подделок могут использоваться современные технологии, при этом зачастую достигаются такое качество и такая точность копирования упаковки, логотипов и элементов защиты, что становится нелегко отличить подделку от оригинального продукта. Распространители поддельного ПО, как правило, привлекают покупателей низкими

ценами, не упоминая о рисках для пользователей, связанных с использованием их товаров. Распространители поддельного ПО также обычно скрывают тот факт, что продают нелицензионный продукт, покупатель которого фактически не приобретает законного права им пользоваться.

4. Компьютерный саботаж или терроризм. Компьютерный саботаж – это умышленное уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя.

Кибертерроризм – это комплексная акция, выражающаяся в преднамеренной, политически мотивированной атаке на информацию, обрабатываемую компьютером и компьютерными системами, создающей опасность для жизни или здоровья людей либо наступления других тяжких последствий, если такие действия были содеяны с целью нарушения общественной безопасности, запугивания населения, провокации военного конфликта. Одним из способов кибертерроризма является политически мотивированная атака на информацию. Она заключается в непосредственном управлении социумом с помощью превентивного устрашения. Это проявляется в угрозе насилия, поддержании состояния постоянного страха с целью достижения определенных политических или иных целей, принуждении к определенным действиям, привлечении внимания к личности кибертеррориста или террористической организации, которую он представляет. Кибертерроризм угрожает не только высокоразвитым в технологическом плане странам, но учитывая динамику развития сети Интернет, и всему миру в целом [5].

5. Компьютерное мошенничество представляет собой умышленное раскрытие информации, замена или искажение данных, хищение чужого имущества или приобретение права на него путем обмана или злоупотребления доверием с использованием компьютерных систем. Наиболее распространены следующие виды компьютерного мошенничества [6]:

– аукционные мошенничества/интернет-мошенничества – например, несуществующая победа на аукционе в интернете, либо на каком-то портале находят товар и рекомендуют его купить, покупатель переводит деньги, но товар не получает;

– мошенничество с банковскими карточками – без ведома человека и без его согласия по его карточке снимаются деньги с его счета;

– мошенничество с кредитными карточками и манипуляции с расчетным счетом – без ведома человека и без его согласия с его расчетного счета производятся денежные операции (сделаны перечисления, оплата кредитной карточкой и т.п.);

– манипуляции с виртуальными счетами/телефонами – по мобильному телефону, не принадлежащему мошеннику, заказаны платные услуги или перечислены на некий виртуальный счет деньги (например, Rate SOL, заказы «Теста смерти», теста IQ, мелодий игр и т.д.).

В связи с тем, что компьютеры и всемирная сеть становятся основными источниками хорошего дохода многих людей, все большее распространение получают различные виды интернет-мошенничества, к которым относятся [6]:

– *фиктивные интернет-магазины*, предлагающие купить товар по низким ценам. Особенно привлекательно это тогда, когда дается возможность купить эксклюзивный товар по заниженной стоимости. Первый способ обмана – требование полной оплаты покупки или ее предоплата до получения. После перечисления денег на счет мошенников, они просто исчезают и не выходят на связь. Второй вариант – это когда оплачивается товар, а взамен покупатель получает или подделку, или какую-нибудь ерунду, которую не заказывал. И снова все попытки связаться с продавцом терпят неудачи.

– *фишинг* – это получение данных чужой платежной карты. Обычно высылаются письма от имени банков или хостингов, на которых заводят электронные кошельки, содержащие информацию о том, что необходимо срочно погасить кредит. Или предлагается по указанной ссылке зайти на сайт банка (выглядеть такая страница будет точно так же, как и реальный сайт, только с небольшими видоизменениями) для ознакомления с изменениями в какой-либо области его деятельности (например, меняется система оплаты и обналичивания средств), где пользователя просят ввести персональные данные с платежной карты. В результате вся информация поступит мошеннику. Так что никогда не следует переходить по подозрительным ссылкам, присланным по электронной почте с неизвестных адресов, и тем более не указывать никаких персональных данных.

– *попрошайки* – виды мошенничества в интернете, которые направлены на человеческую психологию. Точнее говоря, они попросту «давят» на некоторые точки, которые вынуждают людей по собственной воле отдавать свои деньги. Это коварные виды мошенничества и никто не станет писать письма с банальной просьбой «подайте на пропитание». На сайтах или в социальных сетях размещаются объявления с просьбами помочь больному ребенку или сироте. В объявлении, как правило,

указываются все данные для связи и лицевой счет, на который нужно переводить денежную сумму. Вы перечисляете деньги, надеясь, что спасаете жизнь ребенку. Но на самом деле, вы просто пополняете счет какому-то мошеннику.

– *брачная афера* или мошенничества на сайтах знакомств. Они направлены на наивность людей и их отзывчивость. Это довольно популярный способ обмана. Особенно, молоденьких девушек и состоятельных мужчин. Такие виды мошенничества в интернете заняли второе место по «прибыли» и «безнаказанности». Большой популярностью пользуются брачные аферы среди иностранных граждан. В крайнем случае, соотечественников, живущих далеко от злоумышленника. Обычно все начинается с простого знакомства. Это может быть объявление в интернете от лица нетребовательной милой девушки, которая ищет серьезные отношения или же прямое письмо в социальной сети (этот вариант наименее вероятен – мошенника будет довольно легко выследить). Виды мошенничества на сайтах знакомств могут длиться долгий период времени. Обычно такая афера требует 2-3 месяца. После этого периода, наполненного романтикой и любовью, мошенник просит помочь решить финансовые проблемы. Например, дать денег на устройство родителей в пансионат, перевести сумму для перелета к жениху/невесте и так далее. После того как денежные средства попадают на счет, жертва больше не имеет возможности выйти на связь со злоумышленником.

Заключение

В заключение хотелось бы отметить несколько надежных способов, как обезопасить себя и свой персональный компьютер, поскольку каждый из нас в независимости от уровня владения ПК и длительности работы на компьютере, хотя бы раз в жизни становился жертвой компьютерных преступников.

В первую очередь, чтобы не столкнуться с мошенничеством на этапе покупки компьютера необходимо обращаться только в специализированные магазины. Так же обратите особое внимание на гарантийный талон, поскольку вещь дорогостоящая и в случае брака или выхода машины из строя вам гарантированно должны будут его заменить или вернуть деньги, если срок гарантийного талона еще не вышел.

На следующем этапе, при установке программного обеспечения стоит тщательно подходить к выбору данного продукта. На сегодняшний день у каждой компании-разработчиков программного обеспечения существуют нормы упаковки. Перед совершением покупки изучите какой материал использует компания разработчика, что должно быть в упаковке и многие другие характеристики, отличающие лицензированное программное обеспечение от подделки.

Для того чтобы обезопасить себя от вредоносных программ необходимо тщательно подойти к выбору антивирусной программы. Наиболее популярны такие антивирусы, ориентированые с учетом новейших вирусов, как Касперский (KAV), Dr. Web, Avast, 360 Total Security. Но иногда и этого бывает недостаточно. Будьте бдительны и не посещайте сомнительные сайты, не пользуйтесь непроверенными съемными носителями, при скачивании файлов внимательно читайте информацию, которая вам предоставляется.

Так же будьте внимательны при посещении разного рода сайтов на просторах Интернета. Старайтесь не вводить личные паспортные данные, номера телефонов и банковских карт. Не разрешайте подозрительным сайтам использовать ваши данные с других более популярных сайтов. Пользуйтесь более распространёнными ресурсами, на них риск угрозы менее велик.

Будьте осторожны при общении в социальных сетях, не доверяйтесь мало знакомым людям, старайтесь не использовать в разговорах и переписках информацию, не рассчитанную для большого круга лиц. Такого рода вопросы лучше решать при личном контакте с собеседником. Так же будьте осторожны и не верьте всему что написано, до тех пор, пока не убедитесь лично в правдивости информации предоставленной вам.

Старайтесь не совершать покупки в интернет-магазинах, а если уж и возникла такая необходимость, то используйте наиболее популярные сервисы или проверенные интернет-магазины, услугами которых пользовались ваши знакомы.

Соблюдение этих простых правил позволит обезопасить себя и свой компьютер, что в итоге значительно снизит расход денежных средств. Старайтесь быть в курсе часто встречающихся компьютерных преступлений, дабы знать от чего стоит защищать свое IT-устройство.

Литература

1. Электронная библиотека Vizlib [Электронный ресурс] / Интернет-ресурс. – Режим доступа : http://www.pravo.vuzlib.su/book_z2055 _page_17.html.

2. Крылов, В.В. Информационные компьютерные преступления : учебное пособие / В.В. Крылов. – Москва: Юрид. Лит., 2005. – 240 с.

3. Портал «Компьютерные преступления [Электронный ресурс] / Интернет-ресурс. –

Режим доступа : https://sites.google.com/site/komputernyeprestuplenia.

4. Студопедия [Электронный ресурс] / Интернет-ресурс. – Режим доступа : https://studopedia.org/4-77485.htm.

5. Электронная библиотека Kursak.net [Электронный ресурс] / Интернет-ресурс. – Режим доступа : http://kursak.net/kiberterrorizm-i-osobennosti-ego-proyavleniya/

6. Форум [Электронный ресурс] / Интернет-ресурс. – Режим доступа: http://figvam.org

Гром А. В., Ефименко К. Н. Современные киберпреступления и основы кибербезопасности. *Рассмотрены основные виды компьютерных преступлений, вредоносных программ и способы мошенничества в сети Internet, а также даны рекомендации по общим принципам защиты от киберпреступлений.*

Ключевые слова: *компьютерные преступления, вредоносные программы, Internet-мошенничество, безопасность.*

Grom A. V., Efimenko K. N. Modern cybercrime and the basics of cybersecurity*The main types of computer crimes, malicious programs and methods of fraud in the Internet are considered, as well as recommendations on the general principles of protection from cybercrime.*

Keywords: *computer crimes, malicious programs, Internet-fraud, security.*

Статья поступила в редакцию 4 мая 2018 г.
Рекомендована к публикации профессором Павлышом В. Н.

УДК 004.946

Трехмерная реконструкция утраченных памятников архитектуры по фотографическому изображению методом перспективных масштабов

М. П. Руденко
Донецкий национальный технический университет
m.p.rudenko@mail.ru

Руденко М. П. Трехмерная реконструкция утраченных памятников архитектуры по фотографическому изображению методом перспективных масштабов. *В статье рассматривается метод Structure-from-Motion как метод построения трехмерной реконструкции утраченных памятников архитектуры по фотографическому изображению, показаны его положительные стороны и недостатки. На примере построения трехмерной реконструкции дома Юза-Свицына предложен метод перспективных масштабов.*

Введение

Виртуальная реконструкция утраченных памятников архитектуры позволяет сегодня полностью воссоздать их первоначальный облик, применяя последние тенденции в компьютерном моделировании. Процесс создания виртуальной архитектурной среды представляет не только научный интерес, но и историко-культурный, так как приносит вклад в культурное наследие общества.

В настоящее время предлагаются различные методы трехмерной реконструкции различных моделей по фотографическим изображениям. Использование этих методов для реконструкции утраченных памятников архитектуры является особенно интересной задачей, так как зачастую первоначальный облик памятников архитектуры сохраняется только на фотографиях или рисунках, а сам он находится либо в полуразрушенном состоянии, либо полностью утрачен.

Целью данной статьи является рассмотрение метода Structure-from-Motion как метода построения трехмерной реконструкции утраченных памятников архитектуры, а также предложение метода перспективных масштабов на примере виртуального воссоздания дома Юза-Свицына.

Анализ исследований и публикаций

Анализ исследований и публикаций показал большой интерес к теме построения трехмерной реконструкции моделей по фотографическим изображениям [1-4], и не меньший интерес к задачам автоматизации такого построения [5-7].

В [5] рассматривается метод трехмерной реконструкции сцены по фотографическим изображениям Structure-from-Motion (SFM), предложенный в [8]. В [6,7] предложен модифицированный метод SFM, улучшающий качество трехмерной реконструкции модели. Источник [9] также использует метод SFM из [8] и предлагает свой метод построения трехмерной реконструкции модели по фотографическому изображению, ссылаясь на [10-12]. Данный метод трехмерной реконструкции модели был взят как пример для решения задачи построения трехмерной реконструкции утраченных памятников архитектуры, так как решает задачи трехмерного построения архитектурных зданий, используя моделирование, основанное на построении геометрических блоков.

Рассмотрение метода SFM как задачи построения трехмерной реконструкции утраченных памятников архитектуры по фотографическому изображению

В [9] метод SFM встроен в программу трехмерной реконструкции архитектурных зданий по фотографическому изображению “Façade”. Его суть сводится к определению параметров модели и положения камеры таким образом - в программу импортируется фотографическое изображение архитектурного здания, затем сверху на фотографии намечаются основные горизонтальные и вертикальные отрезки для того, чтобы обрисовать форму здания. Эти отрезки в дальнейшем создают трехмерные блоки, которые и формируют модель архитектурного здания.

Задача метода SFM состоит из:

1. Начальной оценки положений камеры и параметров модели, так как архитектурное здание на фотографии расположено в перспективе.
2. Минимизации целевой функции по отношению к параметрам модели и положению камеры для того, чтобы точно определить пропорции и координаты будущей трехмерной модели (рис.1).

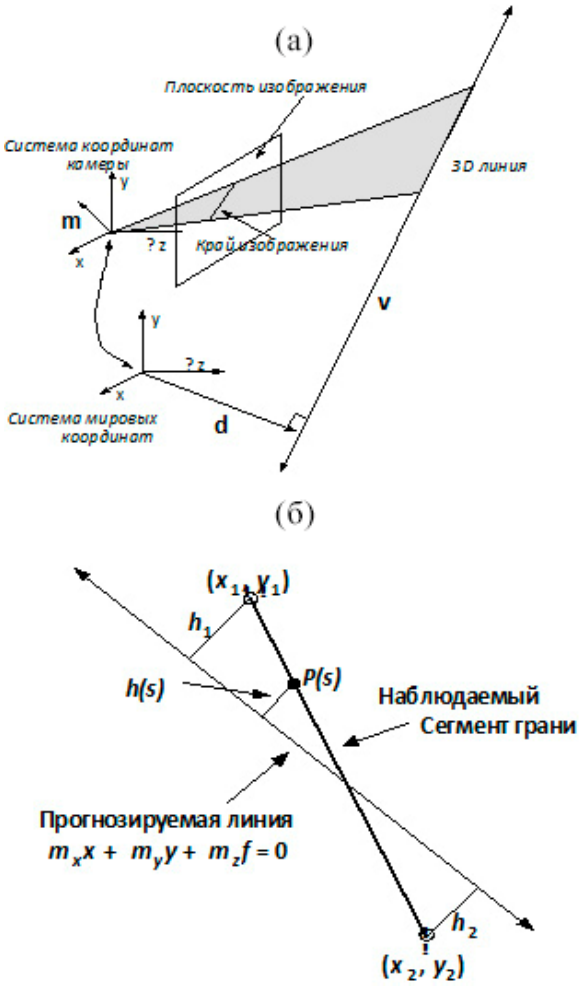


Рисунок 1 – а) Проецирование прямой линии на плоскость изображения камеры; б) Функция ошибки, используемая в алгоритме реконструкции [9].

На рис.1 (а) показано, как прямая линия в модели проецируется на плоскость изображения камеры. Прямую линию можно определить парой векторов v и d, где v – направление линии, а d – точка на линии. Положение камеры относительно мировых координат задается матрицей вращения R_j и вектором сдвига t_j. Тогда вектор нормали, обозначенный буквой m на рисунке, вычисляется из следующего выражения:

$$m = R_j(v \times (d - t_j)) \quad (1)$$

Проекция линии на плоскость изображения представляет собой просто пересечение плоскости, обозначенной m с плоскостью изображения, расположенной в точке $z = -f$, где f - фокусное расстояние камеры. Таким образом, край изображения определяется уравнением:

$$m_x x + m_y y + m_z f = 0 \quad (2)$$

На рис.1 (б) показано, как рассчитывается ошибка между наблюдаемым краем изображения

{(x1, y1), (x2, y2)} и прогнозируемой линией изображения для каждого соответствия. Точки на наблюдаемом краевом сегменте могут быть параметризированы одной скалярной переменной

s ϵ [0, l], где $l = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$ длина края.

Пусть h(s) - функция, которая возвращает кратчайшее расстояние от точки на отрезке p(s) до прогнозируемого края.

При этих определениях полная ошибка между наблюдаемым сегментом края и прогнозируемым краем рассчитывается как:

$$Err_i = \frac{l}{3}(h_1^2 + h_1 h_2 + h_2^2) = m^T (A^T B A) m \quad (3)$$

где:

$$m = (m_x, m_y, m_z)^T$$

$$A = \begin{pmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \end{pmatrix}$$

$$B = \frac{l}{3(m_x^2 + m_y^2)} \begin{pmatrix} 1 & 0.5 \\ 0.5 & 1 \end{pmatrix}$$

Функция (будем называть ее O), которая в итоге рассчитывает натуральную длину края в системе мировых координат является суммой ошибок, т.е. $O = \sum Err_i$.

Так как графический редактор “Facade” является устаревшим, практические вычисления для нахождения натуральных величин отрезков, отмеченных на фотографическом изображении выполняются в графической среде AutoCAD.

Используя данные формулы для построения натуральных величин отрезков в перспективе, необходимо учитывать, что значения матрицы вращения $\boldsymbol{R_j}$ определяется случайным образом и требует не меньше десяти итераций для получения значений, близких к правильным. В [5] предложено несколько методов представления $\boldsymbol{R_j}$, а также сделан вывод о том, что задача представления этого параметра является трудоемкой и требующей длительной работы для получения необходимо значения координат.

При всей простоте расчетных формул данного метода существуют такие недостатки как: поиск удачного значения матрицы вращения; установление фокусного расстояния; зависимость построения натуральных величин отрезков от координатных значений.

Использование метода перспективных масштабов при построении трехмерной реконструкции дома Юза-Свицына

Рассмотренный выше метод SFM определения натуральных величин отрезков, отмеченных на фотографическом изображении натолкнул на мысль о том, что чтобы сам алгоритм работал быстрее и эффективнее, а также требовал меньших затрат при нахождении натуральных величин, необходимо заменить сам метод поиска натуральных величин, который не требует значений матрицы вращения и фокусного расстояния. Таким методом оказался метод построения перспективных масштабов.

Суть этого метода состоит в следующем:

1. Определение и указание точек схода на фотографическом изображении архитектурного здания;

2. Определение и указание натуральных величин отмеченных отрезков на фотографическом изображении методом перспективных масштабов, подробно описанном в [13, С.231-240].

Для практического применения данного метода был выбран частично утраченный памятник архитектуры г. Донецка дом Юза-Свицына. Дом основателя Донецка английского магната Джона Джеймса Юза является истинным памятником архитектуры для нашего города, так как - это одно из первых исторических зданий, спроектированных и построенных в первые годы основания Донецка, выполненное в «кирпичном» стиле, характерном для проектирования общественных и гражданских зданий на рубеже XIX-XX веков (рис.2). Само здание визуально состоит из параллелепипедов, что упрощает построение его трехмерной модели в графической среде AutoCAD.

Алгоритм применения метода перспективных масштабов состоит из следующих пунктов:

1. Импортировать фотографию в рабочую среду графического редактора AutoCAD в начало координат (0,0,0);

2. Наметить точки схода (O_1, O_2);

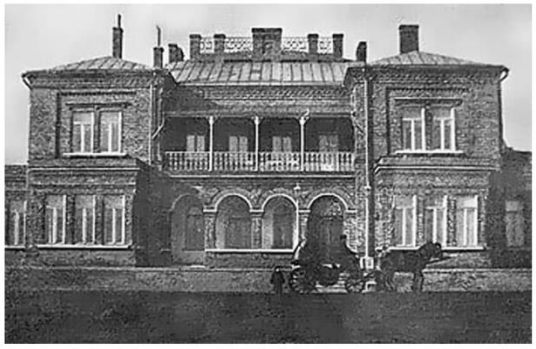
3. Наметить отрезки (AB, BC, BE) на фотографии, натуральные величины которых будут определяться (АкВк, ВкСк, ВкЕк);

4. На основе выполнения пункта 3 последовательно построить трехмерную модель архитектурного памятника.

Так как трехмерная модель дома Юза-Свицына состоит из параллелепипедов, то для определения параметров параллелепипеда требуются только три величины – высота, ширина и глубина (рис.3).

После построения, трехмерная модель архитектурного памятника импортируется в графическую среду 3dsMax, в которой детальнее выстраивается фасад здания, накладывается текстура и конечный вид модели визуализируется (рис.4).

(а)



(б)

(в)

Рисунок 2 – а) Фотография дома Юза, начало XX века; б) нынешнее состояние дома Юза, в) боковой фасад дома [14].

Метод перспективных масштабов является более простым в поиске натуральных величин отрезков, намеченных на фотографии, и дальнейшем построении трехмерной модели по ряду причин:

1. Не требует параметров матрицы вращения камеры, а также параметра фокусного расстояния;

2. Не зависит от координат отрезков;

3. Определяет только пропорциональную зависимость между элементами трехмерной модели, которые потом можно масштабировать.

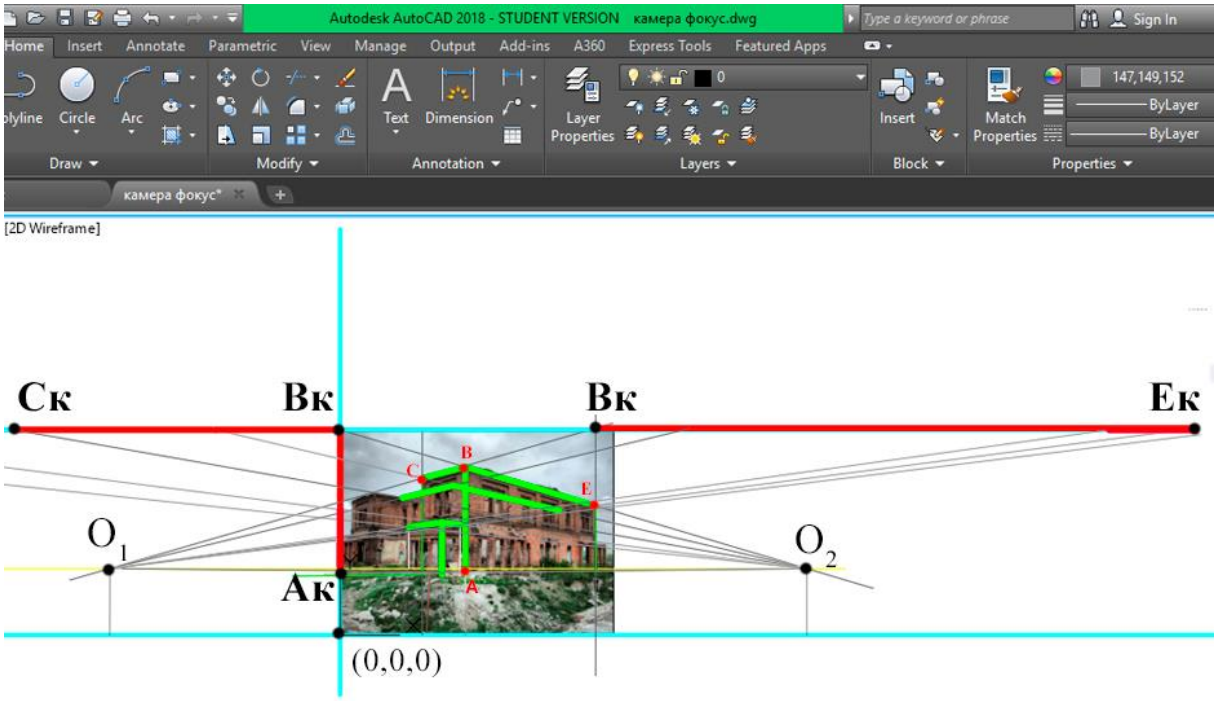


Рисунок 3 – Визуализация метода перспективных масштабов в AutoCAD.

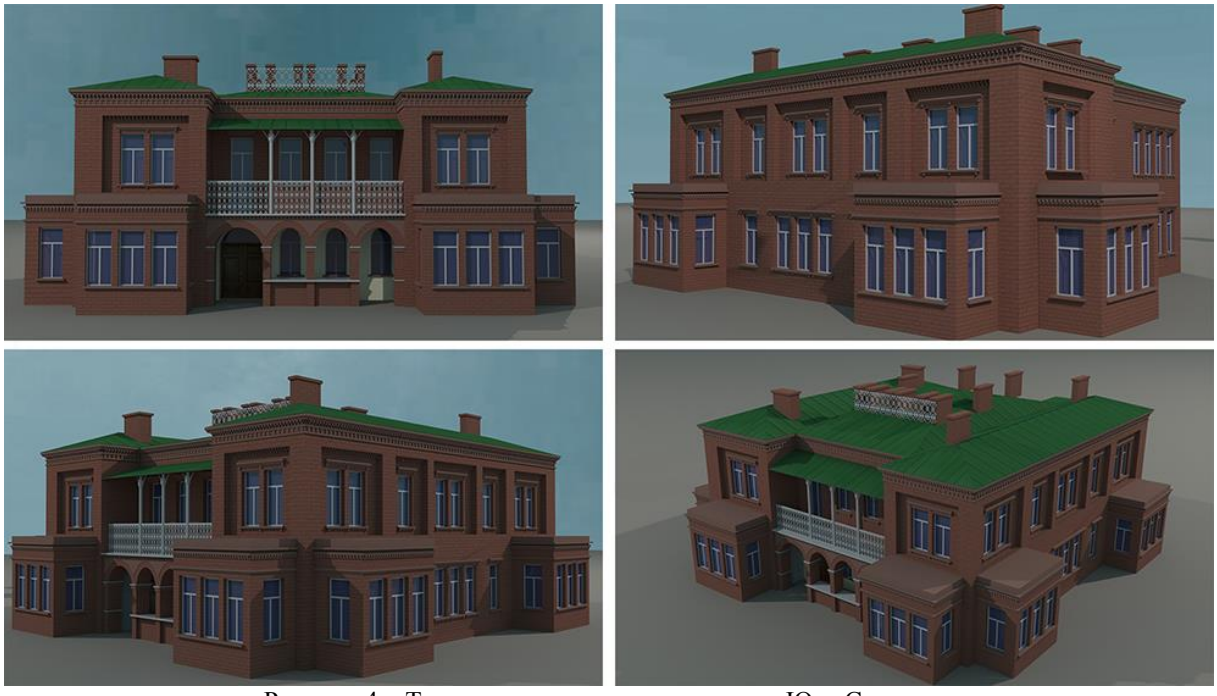


Рисунок 4 – Трехмерная реконструкция дома Юза-Свицына.

Выводы

Рассмотрение метода SFM как метода построения трехмерной реконструкции утраченных памятников архитектуры показало, что при всей простоте формул поиска натуральных величин отрезков, отмеченных на фотографии, такие значения как параметры фокусного расстояния и матрицы вращения камеры, требуют неоднократного поиска и уточнения, что занимает много времени. Предложенный метод перспективных масштабов как метод поиска натуральных величин отрезков, отмеченный на фотографии, является более простым в исполнении, так как не требует вычисления параметров камеры и фокусного расстояния.

Перспективы дальнейшего исследования следующие:

1. Автоматизация метода перспективных масштабов средствами графической среды AutoCAD с использованием встроенного языка

программирования AutoLisp.

2. Использование метода перспективных масштабов для построения более сложных трехмерных объектов, созданных из окружностей, многоугольников и кривых.

Литература

1. Руденко М.П. Методы виртуальной реконструкции памятников архитектуры // Системный анализ и информационные технологии в науках о природе и обществе, № 1(8) – 2(9), 2015. – С. 110-116.

2. Крейдун Ю.А., Жилин С.И. Построение пространственных моделей утраченных архитектурных памятников по одиночным изображениям // Ползуновский вестник, № 3, 2004. – С. 83-88.

3. Меженин А.В., Тозик В.Т. Реконструкция трехмерных моделей по растровым изображениям // Научно-технический вестник информационных технологий, механики, оптики, № 45, 2007. – С. 203-207.

4. Захаров А.А., Тужилкин А.Ю. Трехмерная реконструкция визуальной обстановки по видеоизображениям на основе вероятностного подхода // Радиотехнические и телекоммуникационные системы, № 2, 2014. – С. 45-49.

5. Ковальский С.В., Зори С.А. Исследование алгоритма извлечения трехмерной структуры объектов из их фотоизображений для реконструкции геометрических моделей сцен городских ландшафтов. В кн. Наукові праці Донецького національного технічного університету. Серія: Інформатика, кібернетика та обчислювальна техніка (ИКВТ-2005). Донецк: ДонНТУ, 2005, с.12-21.

6. Ковальский С.В., Зори С.А. Модифицированный алгоритм реконструкции трехмерных сцен городских ландшафтов на основе фотоизображений / Моделирование и компьютерная графика: Материалы I-й Международной научно-технической конференции. – Донецк, ДонНТУ, Министерство образования и науки Украины, 2005. – С. 70-76.

7. Зори С.А., Ковальский С.В. Автоматизация создания трехмерных моделей реальных ландшафтов на основе фотографий // Известия ЮФУ. Технические науки, № 5(106) , 2010. - С. 134-140.

8. Camillo J. Taylor and David J. Kriegman. Structure and motion from line segments in multiple images. IEEE Trans. Pattern Anal. Machine Intell., 17(11), November 1995.

9. Debevec P.E. Modeling and Rendering Architecture from Photographs. Doctoral dissertation. University of California at Berkeley.1996.

10. Camillo J. Taylor and David J. Kriegman. Minimization on the lie group so(3) and related manifolds. Technical Report 9405, Center for Systems Science, Dept. of Electrical Engineering, Yale University, New Haven, CT, April 1994.

11. Eric N. Mortensen andWilliam A. Barrett. Intelligent scissors for image composition. In SIGGRAPH ’95, 1995.

12. Steven Smith. Geometric Optimization Methods for Adaptive Filtering. PhD thesis, Harvard University, Division of Applied Sciences, Cambridge MA, September 1993.

13. Соловьев С.А., Буланже Г.В. Черчение и перспектива. – М.: Высшая школа, 1982. – 319 с: ил.

14. http://all-photo.ru/empire/index.ru.html?kk=2e4b12b045&big=on&img=18604#picts. – Российская Империя в фотографиях.

Руденко М. П. Трехмерная реконструкция утраченных памятников архитектуры по фотографическому изображению методом перспективных масштабов. *В статье рассматривается метод Structure-from-Motion как метод построения трехмерной реконструкции утраченных памятников архитектуры по фотографическому изображению, показаны его положительные стороны и недостатки. На примере построения трехмерной реконструкции дома Юза-Свицына предложен метод перспективных масштабов.*

Rudenko M. P. The lost architectural monuments virtual reconstruction from photograph by the perspective scales method. *The Structure-from-Motion method as the method of the lost architectural monuments virtual reconstruction from photograph is considered, its advantages and disadvantages are shown. The perspective scales method is offered to make the virtual reconstruction of the Hughes-Svitsyn House.*

Статья поступила в редакцию 4 мая 2018 г.
Рекомендована к публикации доцентом Зори С. А.

Инженерное образование

УДК 004.9

Актуальные проблемы подготовки ИТ специалистов в области программной инженерии в высших учебных заведениях РФ

Т. П. Машихина
Волгоградский институт бизнеса, г. Волгоград
Волгоградский государственный социально-педагогический университет, г. Волгоград
tatyana_mashihina@mail.ru

***Машихина Т. П. Актуальные проблемы подготовки ИТ специалистов в области программной инженерии в высших учебных заведениях РФ**. В статье рассматриваются различные факторы, влияющие на качество подготовки выпускаемых высшими учебными заведениями Российской Федерации ИТ-специалистов на примере рассмотрения проблем и специфики преподавания дисциплины «Программная инженерия».*

***Ключевые слова:** федеральный государственный образовательный стандарт, ИТ-специалист, программная инженерия, информатизация, образовательный процесс.*

Введение

Переход российской высшей школы с действовавших государственных образовательных стандартов второго поколения на федеральные государственные образовательные стандарты третьего поколения (ФГОС 3, 3+ и 3++) привел к кардинальному изменению требований к результатам освоения образовательных программ. Отличительной особенностью образовательных стандартов последнего поколения (ФГОС 3++) [1] являются требования к обеспечению качества образования. При этом подразумевается не только внутренняя оценка качества программ, но и процедура внешней оценки, включающей государственную, профессионально-общественную и международную аккредитации.

Еще одним существенным, на мой взгляд, отличием нового поколения стандартов от предыдущего является кардинальное изменение содержания IV раздела стандарта ФГОС: «Характеристика профессиональной деятельности выпускников, освоивших программу бакалавриата». В предыдущем стандарте профессиональная деятельность выпускников была направлена на выполнение широкого спектра научно-исследовательских, педагогических, экспертно-аналитических, политико-управленческих, консультативных и коммуникативных задач в различных сферах общественно-политического, социокультурного и экономического пространства Российской Федерации и мира. В ФГОС 3++ описание области заменено на описание сфер, задач, областей (согласно реестру ПС) профессиональной деятельности «основные области профессиональной деятельности выпускников (в соответствии с Реестром профессиональных стандартов, утвержденным приказом Минтруда России от 29.09.2014 N 667н)». Вместо объектов профессиональной деятельности (п.4.2) приводится механизм определения перечня ПС, требования которых должны быть учтены в программе, а разделы «Виды профессиональной деятельности; разделение на академический и прикладной бакалавриат» (п. 4.3) и «Профессиональные задачи, сформированные виды профессиональной деятельности» (п.4.4.) и вовсе заменены на «Требования к…» (..материально-техническому и учебно-методическому обеспечению программы бакалавриата – п.4.3., кадровым условиям реализации программы бакалавриата – п.4.4, и пр.), что по сути определяет самостоятельное установление объекта (объектов) и задач профессиональной деятельности выпускников, на которые ориентируется программа бакалавриата в образовательной программе.

Таким образом, система высшего образования уже достаточно далеко ушла от жесткого нормирования содержания образования в виде заданного набора дисциплин с фиксированной трудоемкостью (государственные образовательные стандарты ГОС…), что должно способствовать получению высококвалифицированных работников. Однако, возможность «свободного преподавания» еще не означает что вузам удастся сразу создавать квалифицированных специалистов в сфере ИТ, востребованных коммерческими структурами и программами модернизации ведомств и госмонополий. К сожалению, на сегодняшний день, многое, если не большинство, программного обеспечения, которое создается в РФ, все еще «производится», а не точно проектируется, по-прежнему много некачественного программного обеспечения. Проблема подготовки высококвалифицированных специалистов в сфере информационных технологий напрямую связана с наличием серьезного разрыва между количественным и качественным уровнем подготовки выпускаемых вузами специалистов, с точки зрения соответствия требованиям современного ИТ-рынка труда [2]. И на

сегодняшний день без конструктивного участия государства в решении этого вопроса обойтись пока невозможно.

Роль государственной поддержки высшего образования в качестве катализатора развития IT-отрасли

Процесс обсуждения проблем внедрения ИТ в ВУЗах зачастую сводится только к финансовым проблемам ВУЗов, а именно: проблемам несоответствия действующего механизма бюджетного финансирования современным социально-экономическим требованиям и недостаточности бюджетного финансирования высших учебных заведений Российской Федерации, обеспечения финансовой самостоятельности высших учебных заведений Российской Федерации и недостаточных мер государственной поддержки образовательных учреждений в сфере информатизации и пр. Однако, несмотря на то, что главной проблемой, затрудняющей реализацию ИТ-стратегий в ВУЗах, остается недостаток финансирования, стоит заметить, что за последнее десятилетие в России проблемы развития IT-отрасли в целом и подготовки квалифицированных кадров для этой сферы в частности обсуждались неоднократно, в том числе и на самом высоком уровне. Заинтересованность государства в развитии информационных отраслей (будущей основы «экономики, знаний») и поддержка образовательного процесса прослеживается в попытке устранить главные ограничители — недостаточную конкурентоспособность российского сектора исследований и разработок, низкий уровень коммерциализации получаемых научно-технических результатов и слабую заинтересованность бизнеса в поддержке и реализации отечественных инноваций: национальный проект «Образование» (2006—2008 гг.) направленный на внедрение инновационных учебных программ (бюджетное финансирование на сумму 40 млрд. руб.) позволил 57 вузам обновить лаборатории, повысить квалификацию преподавателей, закупить новое оборудование и ПО, дав тем самым первый толчок к модернизации ИТ в вузах; программа создания Федеральных университетов (2007г) позволила оптимизировать региональные образовательные структуры и укрепить в регионах связей между образовательной, экономической и социальной сферами; программа создания Национальных исследовательских университетов — высших учебных заведений (2009г) позволила на более глубоком уровне (бюджетное финансирование 27 вузов в размере до 1,8 млрд. руб. в течение пяти лет) вести образовательную и научную деятельность на основе принципов интеграции науки и образования; пакет постановлений, направленных на развитие взаимодействия между вузами и НИИ с одной стороны и бизнесом с другой (2010г) стимулировал развитие кооперации российских вузов и производственных предприятий (8 млрд. руб. в течении трех лет на поддержку развития инновационной инфраструктуры вузов, а на создание совместных высокотехнологичных производств — 19 млрд. руб.) для использования в реальном секторе потенциала российской высшей школы для подъема наукоемкого производства; «Информационно-телекоммуникационные системы» указом Президента РФ еще в 2011 году были названы среди приоритетных направлений развития науки, технологий и техники в РФ; Государственная программа «Информационное общество (2011–2020 годы)», задачи которой во многом определены основными положениями Стратегии развития информационного общества в Российской Федерации и Концепции долгосрочного социально-экономического развития Российской Федерации на период до 2020 года [3]; а с марта 2012 года действует федеральный закон [4], который ввел в рамки правового поля применение электронного обучения и дистанционных образовательных технологий; Постановление правительства РФ «О мерах государственной поддержки ведущих университетов Российской Федерации в целях повышения их конкурентоспособности среди ведущих мировых научно-образовательных центров» (2013-2017гг) позволило многим вузам (9000000 тыс. рублей в 2013 году, 10500000 тыс. рублей в 2014 году, 10500000 тыс. рублей в 2015 году, 11100155,9 тыс. рублей в 2016 году, 10634121,9 тыс. рублей в 2017 году, 10265628,1 тыс. рублей в 2018 году, 10046879,1 тыс. рублей в 2019 году, 14500000 тыс. рублей в 2020 году) выйти на новый уровень развития и войти в мировой топ-ведущих вузов мира [5]; в целом пакет документов, принятых с 2013 года позволил сделать огромный шаг в области информатизации образовательного процесса вузов; распоряжение правительства РФ [6] с 2014 года по настоящее время способствует формированию региональной информационно-телекоммуникационной инфраструктуры, необходимой для информационного взаимодействия.

В данном документе предложены основные принципы развития информационно-коммуникационных технологий по 12 направлениям в различных сферах социально-экономического развития субъектов Федерации, в том числе в образовании: «В целях модернизации образования для достижения современного качества учебных результатов и результатов социализации рекомендуется развитие на региональном уровне инструментов электронного, в том числе дистанционного, образования с возможностью видеоприсутствия для лиц с ограниченными возможностями. Для повышения качества управления образованием необходимо формирование информационных систем учета обучающихся в образовательных учреждениях.

Для снижения затрат на создание и эксплуатацию однотипных информационных систем в сфере образования целесообразно рассматривать возможность использования "облачных" технологий» [6]. Это дало толчок к созданию программ информатизации муниципальной системы образования и образовательного процесса во всех субъектах РФ (рассчитанных на период до 2020-2021гг).

Таким образом, за последние 10 (11) лет в действиях правительства РФ проглядывает своеобразная логика: сначала упор был сделан на финансировании образовательного процесса, затем началась программа активизации научных исследований, а в данный период времени происходит активное формирование нормативно-правовой базы в сфере информатизации. Очень хотелось бы наедятся, что следующим шагом будет активное содействие (в том числе и финансовое) Минобрнауки в повышении квалификации преподавателей в области современных информационных технологий. Справедливости ради необходимо заметить, что далеко не всем вузам удается планомерно внедрять информационные технологии в связи с тем, что программы поддержки образования разыгрываются по конкурсу между многими вузами, рассчитаны на несколько лет и носят периодический характер. Из-за такой неопределенности учебным заведениям сложно планировать сроки реализации стратегии, она может быть обозначена только на период действия программы. Разумеется, у вузов есть и собственные средства, но остаточное финансирование большинства из них, разбавленное случайными грантами приводит лишь к лоскутной автоматизации. Без вовлечения вузов в научно-практическую деятельность, востребованную коммерческими структурами и программами модернизации ведомств и госмонополий, все проекты информатизации будут отмирать из-за слабой востребованности в учебном процессе.

Проблемы преподавания дисциплины «Программная инженерия»

Однозначно, что проблемы, связанные с преподаванием IT-дисциплин в общем, и дисциплины «Программная инженерия», в частности, существуют не только в России. Нельзя утверждать, что такие проблемы являются широко распространенными, однако статьи в ведущих журналах, личный опыт, беседы с коллегами из разных вузов, чтение различных форумов, приводит неизбежно к выводу, что программная инженерия преподается далеко не эффективно. Рассмотрим, почему, несмотря на достаточную поддержку государства, вариативность в плане составления рабочих программ, качество преподавания дисциплины «Программная инженерия» остается на достаточно низком уровне.

Во-первых, несмотря на предпринятые меры и динамику развития информационных технологий за последнее десятилетие, уровень информатизации образовательного процесса в РФ остается невысоким. И происходит это, в большей степени потому, что, в целом, обеспечение качества IT-образования зависит от постоянной динамики финансовых, технологических, методических, кадровых ресурсов, обеспечивающих образовательный процесс. Эта отрасль требует финансовых затрат на преподавателей иного рода – как только мы начинаем экономить на специалистах, лучшие из них находят работу в другом сегменте рынка труда. В настоящее время, к сожалению, система образования чрезмерно экономна по отношению к специалистам наукоемких специальностей.

Во-вторых, важную роль играет повышение информированности специалистов в сфере ИТ. Мероприятия, направленные на освещение новейших достижений в этой области как правило регулярно проходят, и многие ИТ-компании занимаются этим самостоятельно, однако, как правило, результаты доступны только за достаточно высокую плату, либо только участникам данных мероприятий (в этом случает стоимость самого участия порой равняется 7-10 зарплатам молодого специалиста). Именно здесь и пригодится поддержка государства. Необходима система открытого информационного обмена с внешней средой, а для ее создания требуется организация эффективного механизма вовлечения бизнеса, экспертов, органов государственной власти и ведущих представителей образовательной отрасли в совместную реализацию поставленных задач. Во многих ведущих странах такое взаимодействие организуется путём создания партнёрства государства и бизнеса, которое призвано обеспечить конструктивный диалог поставщиков с государственными органами и образовательными учреждениями.

В-третьих, как правило, в существующих образовательных программах отсутствует сколь-нибудь грамотная корреляция с набором областей знаний выделенных в SWEBOK, хотя еще десять лет назад Комитетом по образованию в области ИТ Ассоциации Предприятий Компьютерных и Информационных Технологий был опубликован русский перевод Software Engineering 2004: Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering («в котором собран всемирный опыт преподавания программной инженерии в университетах и колледжах» [7, с. 5]) под названием "Рекомендации по преподаванию программной инженерии и информатики в университетах".

В-четвертых, SWEBOK выделяет 10 областей знаний: Требования, Проектирование, Конструирование, Тестирование, Поддержка и эксплуатация, Конфигурационное управление, Управление инженерной деятельностью, Процессы инженерной деятельности, Инженерные инструменты и методы, Качество. Конечно прямой перенос SWEBOK на нашу систему образования не возможен, да и не нужен — SWEBOK в данном случае выступает только в роли декларации, списка требований к знаниям. Однако даже в таком сжатом изложении становится ясно, что изучение всех вопросов явно выходит за рамки семестрового преподавания дисциплины.

В-пятых, если кратко выделить основные моменты данного документа "Рекомендации по преподаванию программной инженерии и информатики в университетах", то, перефразируя описание результатов, изложенных в документе SE2004, студент, обученный по специальности «Программная инженерия», должен уметь делать следующее [7, с.29-31]: осуществлять владение знаниями и навыками программной инженерии, необходимыми для того, чтобы приступить к практической работе; работать индивидуально или в группе над созданием качественных программ; производить поиск приемлемых компромиссов в рамках ограничений, накладываемых «затратами, временем, знаниями, существующими системами и организацией»; выполнять проектирование в одной или нескольких предметных областях, используя подходы программной инженерии, объединяющие «этические, социальные, юридические и экономические интересы»; демонстрировать понимание и применение существующих теорий, моделей и методов, необходимых для программной инженерии; демонстрировать такие навыки, как межличностное общение, эффективные методы работы, лидерство и общение; постоянно повышать свою квалификацию - изучать новые модели, методы и технологии по мере их появления.

Однако, перечень требований к результатам освоения Программ бакалавриата, например, по направлению подготовки 09.03.04 Программная инженерия [8, с. 10-15] и 09.03.03. Прикладная информатика [9, с. 7-11] никак не определяют многие области знаний, выделенные в SWEBOK, либо тонко маскируют их под другими понятиями и формулировками.

В-шестых, при преподавании дисциплины «Программная инженерия» не учитывается специфика данной дисциплины, а именно то, что обучение программному обеспечению должно быть сосредоточено на нескольких показателях качества (таких как надежность, масштабируемость, безопасность, доступность, вариативность, удобство использования и пр.), а не на эффективности. Рассмотрим последнюю проблему более подробно.

Специфика преподавания дисциплины «Программная инженерия»

Преподавание дисциплины «Программная инженерия» достаточно сильно отличается от преподавания стандартных дисциплин сферы информационных технологий. Обучение по данной дисциплине должно идти в разрезе сотрудничества, а не соревнования. Например, такие дисциплины как «Информатика», «Базы данных», «Основы программирования» и пр., с их сильными корнями в математике, обычно преподаются с использованием «конвергентного мышления», т.е. перед студентами ставится проблема, имеющая какое-либо правильное решение, и успешные студенты должны стремиться к нахождению этого правильного решения. Многими преподавателями даже создаются комплексы лабораторных работ, решающих одну сквозную задачу на протяжении всего периода обучения по конкретной дисциплине в русле индивидуального и личностно-ориентированного подходов. Несомненно, в плане оценивания и максимально полного донесения знаний до студента данный подход наиболее эффективен. В сфере инжиниринга же, в особенности в области разработки программного обеспечения, требуется дивергентное мышление, где возможны множественные ответы и самые успешные студенты должны найти уникальное, по сравнению с другими студентами, решение. Т.е. преподавателю на занятиях необходимо ставить перед студентами проблемы со множеством решений. Несомненно, при таком подходе присутствует определенная сложность в оценивании каждого студента индивидуально, некоторую сложность привносит и сохраняющийся менталитет (сложившийся за время становления СССР) в сфере плагиата у российских студентов.

Однако, программная инженерия - это совместная дисциплина, процесс обучения студентов данной дисциплине невозможен без сотрудничества. В процессе преподавания различных дисциплин я обратила внимание, что обучение по группам более эффективно на темах, посвященных разработке программного обеспечения. Поэтому, вместо того, чтобы выискивать студентов, списывающих большую часть работы у сокурсников, необходимо поощрять (особенно слабых, отстающих) студентов к тому, чтобы они больше учились, учась вместе. О необходимости особого подхода в плане преподавания дисциплин, изучающих процесс разработки программного обеспечения, говорит и Гарри Поллис [10], оперируя тем, что разработка программного обеспечения имеет фундаментальные характеристики, которые

делают этот процесс особенно сложным для обучения и изучения.

В качестве доказательства своей теории приведу следующие утверждения Гарри Поллиса:

1. Программное обеспечение сильно отличается от физических устройств, разработанных инженерами-механиками. Программное обеспечение является мягким, оно неосязаемо, его нельзя потрогать.

2. Существует мало, если таковые имеются, законов программного обеспечения, которые могут быть универсально применены. Если есть законы программного обеспечения, мы их еще не обнаружили. Несмотря на то что разработчики компьютерного оборудования могут использовать хорошо установленные формулы для вычисления количества тепла, производимого чипами, которые они разрабатывают, разработчики программного обеспечения не достигли консенсуса о том, как измерить свойства своих продуктов, такие как размер программы.

3. Программное обеспечение не производится массово. Процесс изготовления программного обеспечения (например, операционной системы) включает в себя создание копии, а не создание другого идентичного продукта.

4. Спецификации программного обеспечения постоянно меняются, даже в конце цикла разработки. Гарри Поллис приводит следующий пример: «Если вы строите мост, который наполовину завершен, клиент не собирается говорить: «Джи, я подумайте, что мост будет более полезен при следующем повороте реки, а не здесь». К сожалению, такие требования постоянно происходят с программным обеспечением» [10]. Именно поэтому необходимо переосмыслить сам процесс обучения разработки программного обеспечения и то, каких специалистов в результате мы готовим. Ведь, при стандартном обучении, как правило при оценивании различных проектов в области ИТ, домашних и индивидуальных заданий применяются одинаковые или подобные критерии. Но в технике, особенно в сфере разработки программного обеспечения, представление о том, что будет успешным, часто варьируется в зависимости от контекста, включая пользователей, рынок, платформу, дату выпуска и пр.. Это говорит о необходимости дифференцированного оценивания каждого направления работы.

Вместо того, чтобы каждый студент пытался повторить чей-либо опыт воспроизведения какого-либо процесса, и, по сути, заново «изобрести велосипед» изобретенный до него, необходимо предложить перечень различных возможностей для студентов на выбор, разработать модели презентации решения проблемы и указать перечень необходимых условий (реализация, актуальность, практичность, удобство (для интерфейса например), оригинальность графического решения и пр.), объектов, атрибутов, присутствующих/отсутствующих в конечном продукте, и влияющих, в итоге, на общую сумму баллов. Только в этом случае мы сможем создать специалистов в области информационных технологий, востребованных современной экономикой и способных создавать высококачественное программное обеспечение, конкурирующее с западными аналогами на одном уровне.

Литература

1. Программы повышения квалификации 2017 // Координационный совет учебно-методических объединений и научно-методических советов высшей школы / Портал Федеральных государственных образовательных стандартов URL: http://fgosvo.ru/fgosvo/151/150/24/9

2. Барабанов В.Ф., Кенин С.Л., Подвальный С.Л., Сафронов В.В. Актуальные вопросы подготовки высококвалифицированных специалистов в сфере информационных технологий с участием международных компаний // Вестник ВГТУ. 2015. №4. URL: http://cyberleninka.ru/article/n/aktualnye-voprosy-podgotovki-vysokokvalifitsirovannyh-spetsialistov-v-sfere-informatsionnyh-tehnologiy-s-uchastiem-mezhdunarodnyh (дата обращения: 07.11.2017).

3. Постановление Правительства РФ от 15.04.2014 № 313 (ред. от 21.10.2016) «Об утверждении государственной программы Российской Федерации "Информационное общество (2011 - 2020 годы)».

4. Федеральный закон от 28.02.2012 n 11-ФЗ "О внесении изменений в закон российской федерации "Об образовании" В части применения электронного обучения, дистанционных образовательных технологий" (принят гд фс РФ 14.02.2012).

5. Постановление Правительства от 16 марта 2013 г. № 211 «О мерах государственной поддержки ведущих университетов Российской Федерации в целях повышения их конкурентоспособности среди ведущих мировых научно-образовательных центров» (с изм. в ред. Постановлений Правительства РФ от 30.12.2013 г. №1311, от 26.12.2014 г. № 1519, от 22.05.2015 г. №491, от 9.04.2016 г. № 287, от 10.02.2017 г. №171).

6. Распоряжение Правительства РФ от 29.12.2014 N 2769-р (ред. от 03.03.2017) «Об утверждении Концепции региональной информатизации» (с изм. в ред. Постановления Правительства РФ от 03.03.2017 N 256)

7. Рекомендации по преподаванию программной инженерии и информатики в университетах = Software Engineering 2004: Curriculum Guidelines for Undergraduate Degree Programs in Software Engineering; Computing Curricula 2001: Computer Science: пер. с англ. — М.: ИНТУИТ.РУ «Интернет-Университет

Информационных Технологий», 2007. — 462 с. : ил.

8. Приказ Об утверждении федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 09.03.03 Прикладная информатика // Координационный совет учебно-методических объединений и научно-методических советов высшей школы / Портал Федеральных государственных образовательных стандартов URL: http://fgosvo.ru/uploadfiles/FGOS%20VO%203++/Bak/090303_B_3_17102017.pdf

9. Приказ Об утверждении федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 09.03.04 Программная инженерия // Координационный совет учебно-методических объединений и научно-методических советов высшей школы / Портал Федеральных государственных образовательных стандартов URL: http://fgosvo.ru/uploadfiles/FGOS%20VO%203++/Bak/090304_B_3_17102017.pdf

10. Gary Pollice, Teaching software development vs. Software engineering // IBM Corporation 2005. Dec. 2005. URL: https://www.ibm.com/developerworks/rational/library/dec05/pollice/pollice-pdf.pdf

Машихина Т. П. Актуальные проблемы подготовки ИТ специалистов в области программной инженерии в высших учебных заведениях РФ*. В статье рассматриваются различные факторы, влияющие на качество подготовки выпускаемых высшими учебными заведениями Российской Федерации ИТ-специалистов на примере рассмотрения проблем и специфики преподавания дисциплины «Программная инженерия».*

Ключевые слова: *федеральный государственный образовательный стандарт, ИТ-специалист, программная инженерия, информатизация, образовательный процесс.*

Mashikhina T. P. Actual problems of training of IT specialists in the area of programmatic engineering in higher educational institutions of the Russian Federation *The article discusses various factors affecting the quality of higher education institutions of the Russian Federation it professionals for example, consideration of problems and the specifics of teaching the discipline "Software engineering".*

Keywords: *federal state educational standard, IT- expert, software engineering, informatization, educational process.*

Статья поступила в редакцию 23 мая 2018 г.
Рекомендована к публикации профессором Миненко А. С.

УДК 378.147

Использование персональных сайтов преподавателей для дистанционного обучения

И. Ю. Анохина, Т. В. Кучер
Донецкий национальный технический университет
ingatula@mail.ru

Анохина И. Ю., Кучер Т. В. Использование персональных сайтов преподавателей для дистанционного обучения. *Статья посвящена актуальной проблеме современного образования – дистанционному обучению. Рассматриваются возможности создания личных сайтов преподавателей, сравниваются такие системы управления контентом сайта как Wordpress, Ucoz, Google Sites, Wix. Анализируются достоинства и недостатки систем именно с точки зрения разработки сайтов для учебных целей. Даны рекомендации по выбору систем управления сайтом.*

Ключевые слова: *дистанционное обучение, Wordpress, Ucoz, Google Sites, Wix, дистанционный портал, личные сайты преподавателей.*

Введение

Под дистанционным обучением понимается учебный процесс, при котором все или часть учебных занятий осуществляется с использованием современных информационных и телекоммуникационных технологий. Наличие обучающих дистанционных курсов на данный момент является неотъемлемой частью информационно-образовательной среды.

Дистанционное обучение не вступает в противоречие с традиционным образованием, а дополняет, обогащает, модифицирует его. Применение технологий дистанционного обучения позволяет расширить возможности обучения по многим критериям: формируется единое информационное пространство, появляется возможность обучения без отрыва от работы, улучшается качество восприятия материала, т.к. вместо конспектов лекций студенты имеют возможность читать полный авторский курс.

Ведущие вузы мира ведут разработки в этом направлении. В 2012 году был запущен совместный проект Гарвардского университета и Массачусетского института технологии (MIT), получивший название edX course, целью которого является предоставление бесплатных on-line курсов для всех желающих, вне зависимости от уровня подготовки и местонахождения [1,2]. Для записи на курсы достаточно зарегистрироваться с указанием электронной почты. Если вы собираетесь получить сертификат об окончании курса, то фамилию и имя желательно указать настоящие, если сертификат не нужен, можно использовать псевдоним.

Казалось бы, зачем лучшим вузам мира бесплатные курсы? Вполне достаточно желающих учиться платно. Во-первых, это популярность, во-вторых, возможность отбирать талантливых абитуриентов во всех странах мира, в- третьих, прекрасная реклама уровня преподавания.

Одним из вариантов дистанционного обучения Рунета можно назвать Национальный Открытый Университет «ИНТУИТ» [3]. Сайт содержит несколько сотен открытых образовательных курсов по тематикам компьютерных наук, информационных технологий, математике, физике, экономике и другим областям современных знаний. По прохождении курсов можно бесплатно получить электронный сертификат. Также возможно платное получение сертификатов о повышении квалификации. Кроме того, организация действует как издательство, выпуская учебную литературу по курсам.

14 сентября 2015 года восемь ведущих вузов России презентовали Национальную платформу открытого образования, которая сегодня официально начала работать на портале https://openedu.ru [4]. Первоначально были выложены 46 курсов, на данный момент их количество увеличилось до 233. Курсы выкладываются преподавателями ведущих российских вузов − МГУ, НИТУ МИСиС, СПбГУ, СПбПУ, НИУ «ВШЭ», МФТИ, ИТМО и УрФУ.

«Открытое образование» − современная образовательная платформа, сочетающая в себе лучший опыт зарубежных коллег и инновационные методы обучения.

«Предполагается три варианта использования курсов, первый – это дополнительный высококачественный контент, второй – курсы, которые являются частью образовательных программ для вузов, и третий – курсы, которые сможет освоить каждый желающий» [5].

Таким образом, технологии дистанционного обучения являются признанным компонентом образования, который используют все большее число учебных заведений.

Постановка проблемы

Длительное время вузы использовали систему дистанционного образования Moodle. Не останавливаясь на ее достоинствах/недостаткам, отметим, что Moodle считается системой закрытого типа, т.е. для работы в системе требовались логин и пароль, выдаваемый администратором составителю курса, который в свою очередь записывал на курс учащихся. Не имея пароля и логина, изучать курс невозможно.

На данный момент система уступает позицию первенства системам открытого образования, хотя многие вузы еще продолжают ее использовать. Это понятно. Жаль потерять сделанные наработки, ведь те же тесты, увы, изъять из Moodle не удастся.

В 2009г. было создано Региональное Северокавказское отделение Объединенного фонда электронных ресурсов «Наука и образование». Донскому государственному техническому университету было поручено ведение Северокавказского отделения объединённого фонда электронных ресурсов. На базе Moodle был создан портал СКИФ. Часть курсов этого портала находятся в свободном доступе, часть в закрытом [6].

Кафедра прикладной математики ДонНТУ уже много лет ведет курсы на факультете повышения квалификации для преподавателей вуза. Один из курсов – «Внедрение в образовательный процесс современных информационных технологий». Целью курса является разработка личных сайтов преподавателей вуза и наполнение их информацией.

Много лет назад мы использовали технологию HTML, так называемое «создание сайта по кирпичикам». Преподаватели создавали свои сайты, используя язык гипертекстовой разметки. Учитывая, что на курсах обучались преподаватели разного уровня подготовки в области IT – технологий, сайты получались разного уровня сложности и оформления.

С возникновением и распространением Систем управления содержимым (контéнтом) сайта (англ. Content management system) CMS задачи значительно упростились.Однако, систем такого вида много и возник вопрос определения, какая именно из систем наилучшим образом подходит под размещение учебных электронных курсов.

Таким образом, нами была **поставлена задачи определить оптимальную с точки зрения сервиса, удобства и простоты использования, а также возможностей** систему управления контентом сайта, причем сайта, создаваемого именно для учебных целей и преподавателями, которые не являются профессионалами в сфере IT – технологий.

Все рассматриваемые системы предполагают возможность бесплатного использования.

Исследования

В процессе работы сравнивались системы Wordpress, Ucoz, Google Sites, Wix. В каждой из них нами создавались учебные сайты, проводился анализ удобства работы в системе, ее возможностей.

Были сформулированы критерии, по которым оценивалась каждая CMS:

простота обучения, т.е. возможность использования системы без дополнительной документации, причем для пользователей с разным уровнем знаний;

удобство панели администратора;

качество и количество готовых шаблонов, возможность их редактирования;

наличие плагинов;

количество и качество предоставляемой статистики;

«хороший» адрес сайта, т.е. такой, который можно достаточно легко запомнить, т.к. пройдет определенное время, прежде, чем сайт станет появляться на первых страницах поисковиков;

безопасность сайта, вероятность его удаления;

работа с библиотекой файлов, размещаемых на сайте, их допустимые форматы.

На рис.1 показан личный сайт автора (http://tatyanakucher.ucoz.ru), а на рис.2 – разработанные в этой системе, сайты преподавателей ДонНТУ (http://gaidaroleg.ucoz.ru, рис. 2, цифра 1; http://evolkova.ucoz.net, рис. 2, цифра 2). Как видим, у Ucoz достаточно возможностей для размещения материала для занятий, кроме этого сервис достаточно дружелюбен (в отличие от других сервисов) к чужим разработкам, на сайт можно добавлять различные виджеты от Яндекс, Google и др.

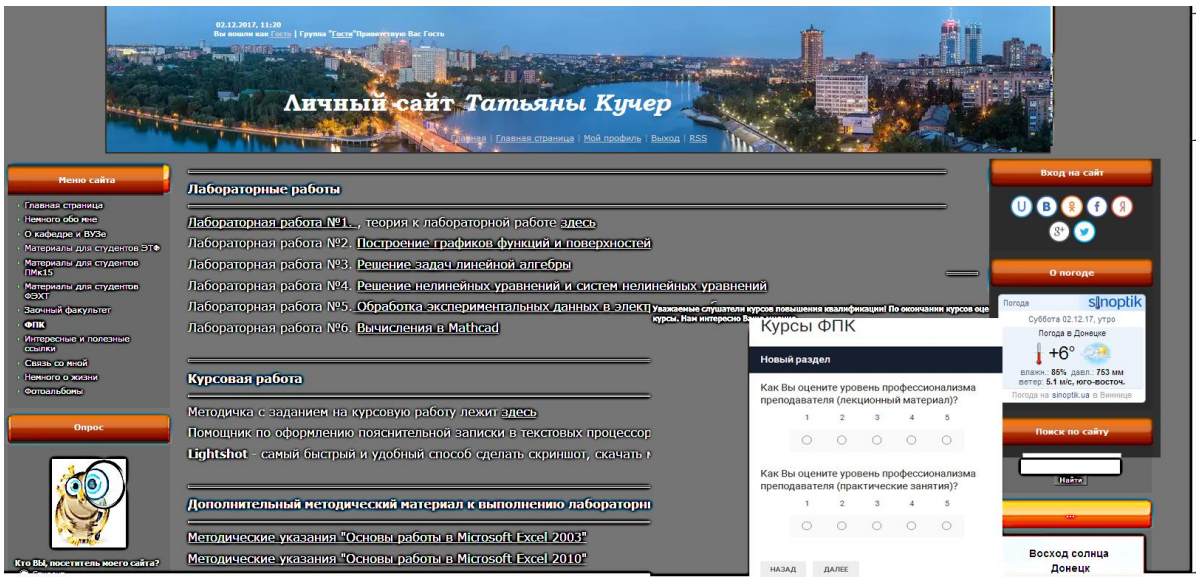


Рисунок 1 – Сайт Т.В. Кучер

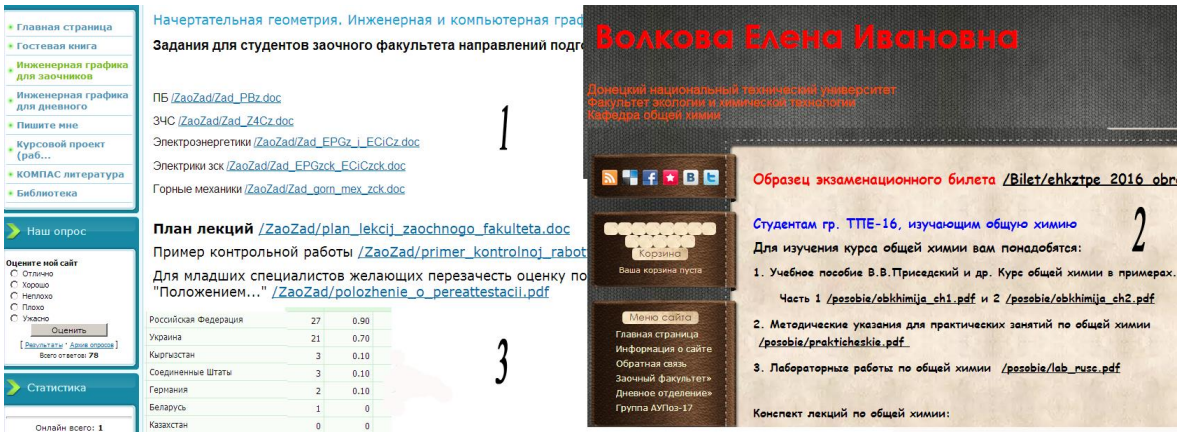


Рисунок 2 – Сайты преподавателей ДонНТУ, созданные в Ucoz

Что можно отнести к недостаткам Ucoz. Во-первых, сложность работы в качестве администратора с точки зрения новичка-разработчика. Также если сайт открыт в режиме администрирования, то через полчаса, если вы в нем не работаете, появляется сообщение «Доступ запрещен. Истек период сессии». Ясно, что преподаватель, размещая материалы лекций, может прерваться и внести дополнения в публикуемый материал. Более того, при повторном открытии браузера, допустим, на следующий день, система Wordpress не требует пароля, если, конечно, сайт открывается с одного и того же компьютера. Для Ucoz пароль следует вводить вновь.

Цифрой 3 на рис.2 обозначена предоставляемая статистика. Информацию можно собирать по дням, месяцам, по странам. В отличие от системы WordPress, предоставляющей красивые диаграммы и графики, данные выводятся только таблично без детализации.

Существенным недостатком системы является то, что в соответствии с соглашением, заключаемым пользователем, т.е. создателем сайта и Обществом с Ограниченной Ответственностью «Юкоз Медиа» «…при использовании сервиса на безвозмездной основе и в случае признания Аккаунта неиспользуемым, Лицензиат вправе приостановить оказание услуг».

К сожалению, нашим преподавателям пришлось столкнуться с этой проблемой в 2014г., когда созданные весной сайты за лето были признаны неиспользуемыми и удалены. Переписка с технической службой Ucoz к восстановлению сайтов не привела.

Проанализировав те недостатки, которые оказались для нас наиболее существенными (сложность управления, возможность удаления сайта, навязчивая реклама), мы пришли к выводу замены платформы.

Следующий опыт касался создания сайтов в системе Google Sites.

Сразу отметим простоту использования CMS. Даже самые далекие от IT – технологий

преподаватели с удовольствием создавали сайты. Нет временных ограничений на использование, т. е. ваш сайт не удалят, если вы сами этого не захотите.

На рис. 3 цифрой 1 показан режим заполнения страницы сайта. Панель инструментов напоминает панель форматирования в Word. Цифра 2 – действия над страницами (удалить, добавить, редактировать), а также переход в режим управления макетом сайта. Цифра 3 рисунка – управление сайтом.

Пользователи отмечают следующие недостатки сайтов Google:

- ✓ неудобный для запоминания адрес;
- ✓ отсутствие CSS и JavaScript;
- ✓ частичное редактирование дизайна, пользователь сможет форматировать лишь цветовую гамму, изменять размером или шрифт [7,8];

трудности в подключении Яндекс или Google метрик, более того информеры Яндекс метрики неточно отображают информацию посетителям, хотя в режиме администрирования таких проблем не возникает.

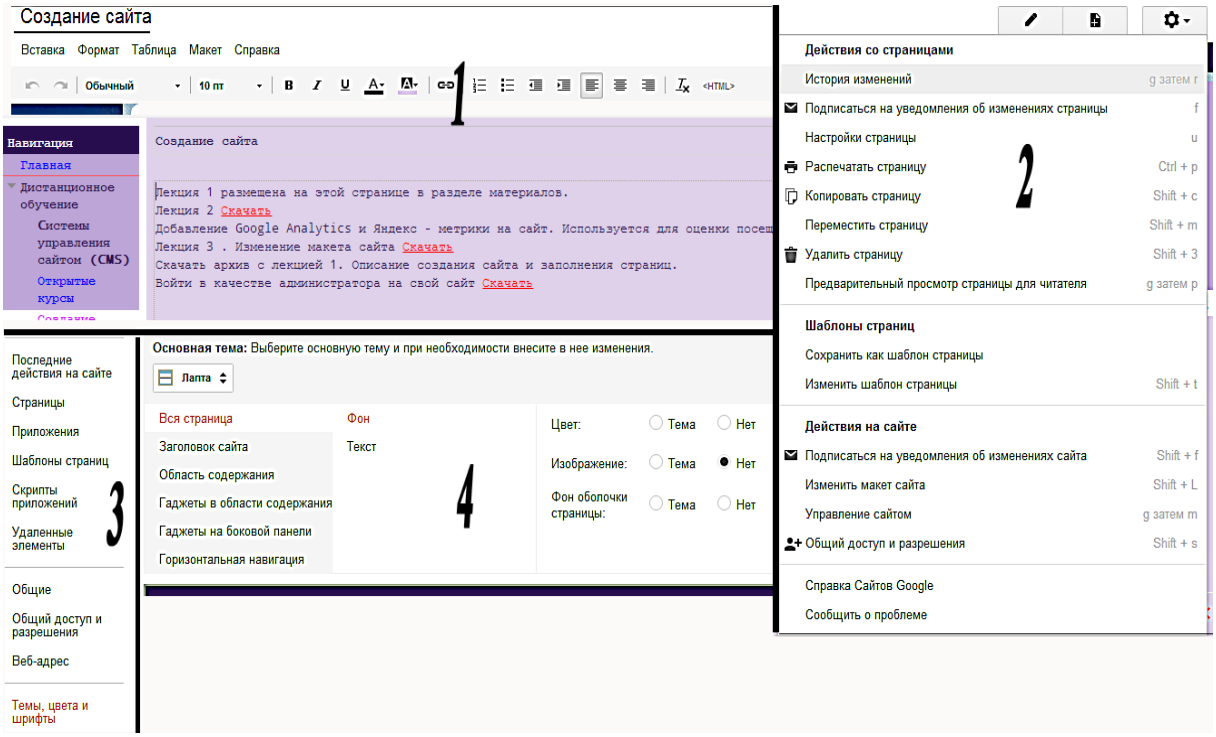


Рисунок 3 –Google Sites. Режим администрирования

Google запустил Google Sites в 2008г. В 2010г. были расширены возможности системы. Теперь можно добавлять календарь (Google Calendar), список задач (Google Tasks) и документы из Google Docs.

В 2016г в Google Sites появился более удобный визуальный редактор с возможностью совместного редактирования. Это позволяет организовать командную работу, так как в этом случае администратор может назначать права доступа, закрепляя страницы за пользователями. На страницы сайта можно вставлять документы карты Google Maps. Разработаны адаптивные шаблоны, которые хорошо отображаются на телефонах, планшетах и широких мониторах[9].

На рис. 4 слева сайт Кучер Т.В. (https://sites.google.com/site/tatyanaviktkucher/) и преподавателей кафедры «Физика» (https://sites.google.com/site/0702907mts/).

При всех перечисленных недостатках, простота, удобство использования позволяют использовать систему именно для не столь сложных учебных сайтов. В целом если нужен вариант быстро создаваемого, легко редактируемого сайта, без так называемых, «наворотов», то для непрофессионалов, на наш взгляд, это один из лучших и простых вариантов. Авторами были разработаны сайты и в Wordpress [10, 11]. На рис. 5 показан сайт Анохиной И. Ю. (innaanohina.wordpress.com, цифра 1 рисунка).

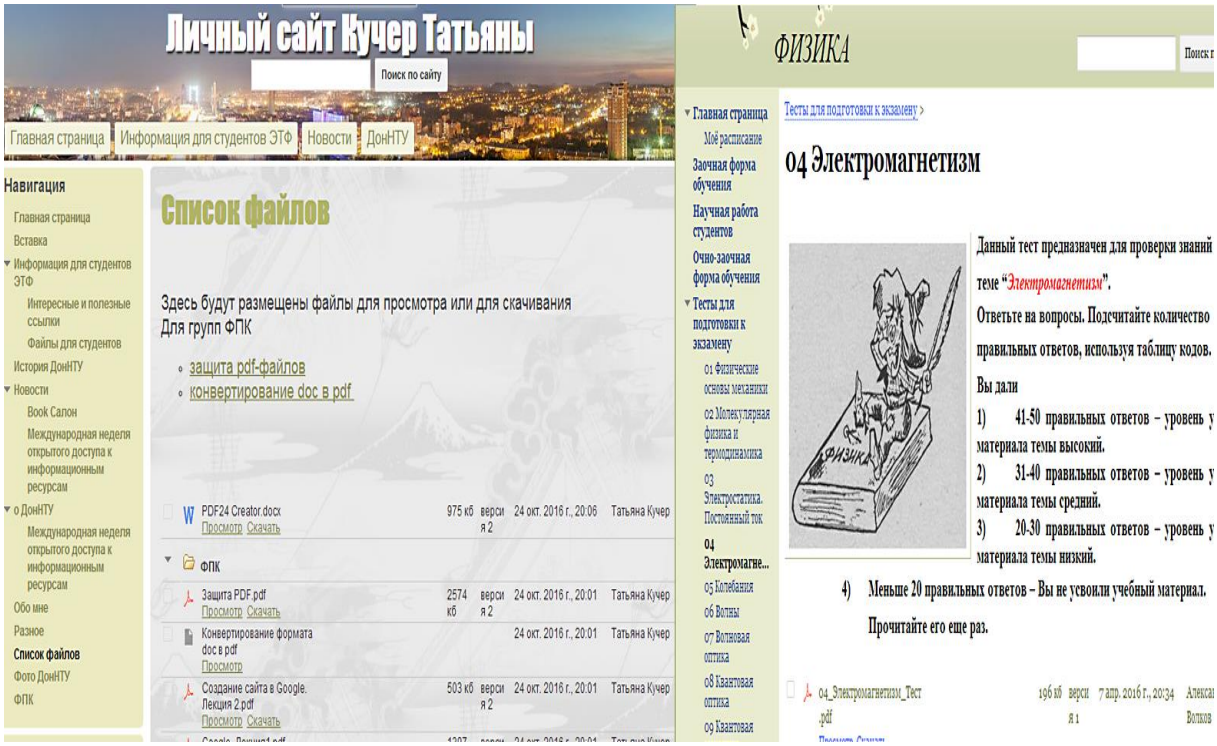


Рисунок 4 – Сайты, созданные в Google Sites

Wordpress позволяет легко размещать файлы с учебными материалами, как в библиотеке, так и использовать ссылки на размещенные в других местах материалы.

В частности, большинство материалов авторов размещены в облаке электронной почты. В библиотеке можно размещать документы, видео, аудио файлы и файлы изображений. При необходимости использовать другие форматы, мы используем облачные технологии.

Цифрой 2 на рисунке показана собираемая Wordpress статистика, которая на наш взгляд здесь является одной из лучших среди исследуемых CMS. Кроме стандартной статистики по количеству посещений и посетителей, дается список стран, из которых шли обращения к сайту (цифра 3 рисунка), а также список наиболее популярных страниц сайта.

Цифрой 4 нами обозначена лишь часть доступных виджетов, а цифрой 5 – статистика отсеянного спама. Систему Wordpress можно рекомендовать для использования, она предоставляет достаточно возможностей и в то же время удобна в эксплуатации. Отметим, что Wordpress для оформления сайта на данный момент предлагает 498 тем, из них 298 – бесплатных.

Личные сайты преподавателей, являясь, безусловно, удобным вариантом организации дистанционного обучения, в первую очередь являются рекламой самого автора – преподавателя, а не кафедры, вуза в целом. Поэтому мы решили разработать дистанционный портал кафедры и оценить возможности применения его в учебном процессе. Портал создавался в системе Wix.

Нами ставилась задача разместить учебные материалы преподавателей кафедры по разным дисциплинам на одном сайте. Пока жестких требований к внешнему виду не предъявляется, т.к. параллельно ведется опрос студентов, какие страницы удобны для работы, почему, есть ли замечания к дизайну. Цифрой 1, рис. 6 отмечена главная страница сайта (https://pmdonntu.wixsite.com/portal), цифры – 2, 3 – образцы страниц, на которых размещены курсы «Математический анализ» и «Теория вероятностей». Следует отметить несомненное достоинство системы, Wix позволяет посмотреть, как будет выглядеть сайт на мобильном устройстве и ввести дополнительные функции для улучшения качества просмотра страниц сайта в этом режиме. На данный момент конструктор Wix считают одним из лучших русскоязычных конструкторов. Богатство функционала, простота, качественный дизайн, богатый магазин приложений [13].

Рисунок 5 – Возможности Wordpress

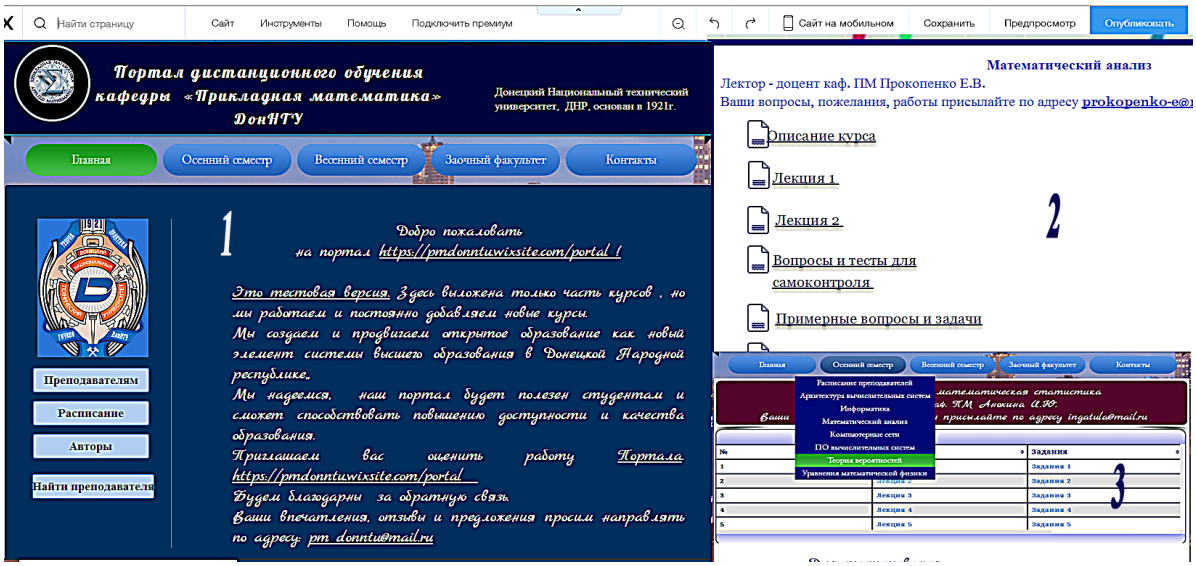


Рисунок 6 – Дистанционный портал кафедры «Прикладная математика» [12]

Однако, мы не можем пока рекомендовать систему Wix только потому, что портал на этой платформе существует всего два месяца. Нами ранее был создан сайт в системе UMI, первоначально к работе сайта не имелось претензий, но, когда количество посетителей увеличилось, нам предложили или перейти на платный тариф, или убрать все ссылки на сайте(!), оставив только ссылки на государственные учреждения. Ясно, что для сайта, содержащего большое количество ссылок на учебные материалы, бесплатный вариант уже не подходил. Мы сделали вывод, что разработчики UMI (компания «Юмисофт») ожидают, когда сайт раскрутится и после этого своими изменившимися требованиями ставят создателей сайта перед условием «или плати, или теряй сайт». Мы перестали работать с этой системой, однако теперь, прежде чем рекомендовать новую платформу, проверяем каждую CMS не менее полугода.

Выводы

Дистанционное обучение обладает такими преимуществами как доступность, технологичность, универсальность, эффективность, модульность, параллельность, отвечает требованиям современной жизни. Этим обусловлен постоянно повышающийся интерес как к самому образованию, так и к средствам его реализации.

В статье рассматривался вопрос поиска оптимальных систем управления контентом CMS для размещения учебных материалов как одного преподавателя, так и подразделения. Как показали исследования, если необходимо создать строгий, классический портал, то оптимальным будет выбор WordPress. Для преподавателей, далеких от IT –технологий, лучше использовать систему Google Sites, которая хотя и менее функциональна, зато проста в использовании. Для тех, кто ценит дизайн, элегантность и современность, нам кажется наиболее подходящей система Wix, обладающая богатым функционалом, современным дизайном и легкостью в использовании.

Литература

1. Harvard University. Online learning. Режим доступа: http://online-learning.harvard.edu/courses?sort_by=date_added&cost%5B%5D=free

2. Massachusetts Institute of technology. MITOpenCourseWare. Режим доступа: https://ocw.mit.edu/index.htm

3. Национальный Открытый Университет "ИНТУИТ" | Бесплатное образование. Режим доступа http://www.intuit.ru/

4. Открытое образование. Курсы ведущих вузов России. Для каждого без ограничений. Режим доступа: https://openedu.ru

5. 8 Крупных вузов основали российскую платформу открытого образования/Наука и технологии России — STRF.RU. Режим доступа: http://www.strf.ru/material.aspx?CatalogId=221&d_no=96104#.WiI4ySmin3F

6. Электронная информационно-образовательная среда ДГТУ. СКИФ. Режим доступа: http://skif.donstu.ru

7. Недостатки конструктора сайтов Google Sites. HostComp.ru. Hi-Tech новости и технологии. Режим доступа: https://www.hostcomp.ru/nedostatki-konstruktora-saytov-google-sayty.html

8. Анохина И.Ю. Сравнительный анализ систем управления контентом сайтов для дистанционного обучения, Информатика и кибернетика, № 1. – Донецк: ДонНТУ, 2015, с.35-43.

9. Обзоры и новости о Google Sites. LiveBusiness. Режим доступа: http://www.intranetno.ru/tool/409/

10. Личный сайт Анохиной И.Ю. Режим доступа: innaanohina.wordpress.com

11. Личный сайт Кучер Т.В. Режим доступа: kuchertatyana.wordpress.com

12. Дистанционный портал кафедры «Прикладная математика». Режим доступа: https://pmdonntu.wixsite.com/portal

13. Сравнение конструкторов сайтов uCoz и Wix. SITE-BUILDERS. Режим доступа: https://site-builders.ru/ucoz-vs-wix

Анохина И. Ю., Кучер Т. В. Использование персональных сайтов преподавателей для дистанционного обучения. *Статья посвящена актуальной проблеме современного образования – дистанционному обучению. Рассматриваются возможности создания личных сайтов преподавателей, сравниваются такие системы управления контентом сайта как Wordpress, Ucoz, Google Sites, Wix. Анализируются достоинства и недостатки систем именно с точки зрения разработки сайтов для учебных целей. Даны рекомендации по выбору систем управления сайтом.*

Ключевые слова: *дистанционное обучение, Wordpress, Ucoz, Google Sites, Wix, дистанционный портал, личные сайты преподавателей.*

Anokhina I. Yu., Kucher T. V. Use of personal sites of teachers for distance learning. *The article is devoted to the actual problem of modern education - distance learning. We consider the possibility of creating personal sites of teachers, we compare such content management systems as Wordpress, Ucoz, Google Sites, Wix. The advantages and disadvantages of systems are analyzed precisely from the point of view of developing websites for educational purposes. Recommendations for the choice of site management systems are given.*

Keywords: *distance learning, Wordpress, Ucoz, Google Sites, Wix, remote portal, personal sites of teachers.*

Статья поступила в редакцию 17 мая 2018 г.
Рекомендована к публикации профессором Павлышом В. Н.

УДК 004.8

Исследовательская работа студентов, как образовательная составляющая подготовки медицинского специалиста среднего звена

О.В. Швыдкий, Л.А. Момоток
Донецкий медицинский колледж
lmomotok@yandex.ru.

Швыдкий О. В., Момоток Л. А. «Исследовательская работа студентов, как образовательная составляющая подготовки медицинского специалиста среднего звена». *В статье рассматривается исследовательская работа студентов на лечебной базе Республиканского онкологического центра (РОЦ), где использованы информационные технологии для диагностики и лечения онкологических больных. Используя элементы проектного обучения в малых подгруппах, наблюдая и анализируя исследуемые объекты, исследовательская работа, рассматривается в системе личностно-ориентированного образования и направлено как на индивидуальный поиск истины, так и коллективный. В статье воспроизведены методики последовательного ознакомления обучающихся в идее дидактических таблиц с обязательными этапами исследовательской работы, которые помогают среди потоков научной информации выбирать самое ценное для проведения системного анализа.*

Ключевые слова: *медицинская информация, медицинские приборно-компьютерные комплексы (МПКК), визуальные методы диагностики, предлучевая подготовка, системы дозиметрического планирования (СДП), топометрические процессы, рентгеновский симулятор, лучевая терапия, линейный ускоритель.*

Введение

При подготовке медицинских работников среднего звена значение исследовательской работы (ИР) в образовательном процессе студентов, как особого вида поисков истины, велико. Основы ИР должны быть переданы молодёжи именно в студенческие годы. Эти умения могут понадобиться студентам в дальнейшем, а могут и не понадобиться, главное, чтобы они были усвоены, опробованы сейчас, чтобы на изучение методик в будущем не было затрачено драгоценное время, когда специалист состоится. Исследовательская работа учит студентов готовности к постоянному самообразованию и самосовершенствованию, повышению квалификации. Исследовательская работа на лечебных базах, оснащённых информационными технологиями, должна проводиться со студентами старших курсов на конечном этапе изучения информатики, когда получены основы медицинских знаний и ощущается потребность в получении новых сведений о современных компьютерных технологиях в медицине. Именно информационные дисциплины способны заинтересовать, увлечь молодёжь осознанно знакомиться с интеграцией компьютерных технологий в медицину, что прогнозирует высокий эффект усвоения и закрепления знаний, в результате чего постижение всех тонкостей информационной поддержки лечебно-диагностического процесса становится понятным и интересным.

Посвятить молодёжь в исследовательскую работу – главное назначение преподавателя. Преподаватель - это исследователь. Он обязан развивать у студентов важное направление исследовательской работы – умение наблюдать и анализировать исследуемый объект, получать новые знания, выдвигать гипотезы и проверять их научным путём [1]. Исследовательской работой надо заниматься постоянно, как составляющей образовательного процесса. И не важно, как будет проводиться ИР – сопровождать учебный процесс или проходить самостоятельно, целенаправленно, как научно-исследовательская деятельность с отдельными студентами. Необходимо время, чтобы убедится в правильности выбора методик ИР, подобрать лучший алгоритм для групп с разным уровнем подготовки студентов. Важно, чтобы студентам было интересно, чтобы положительные эмоции от собственного успеха в обучении способствовали творческим поискам. Хорошие идеи появляются в результате многократных совместных обсуждений не сразу. Исходя из многолетнего опыта работы, лучшим вариантом является постепенное введение обучающейся молодёжи в ИР. То есть, первый этап должен быть обязательным при проведении практических занятий на лечебных базах, где преподаватель знакомит студентов с элементами исследовательской деятельности в учебном процессе. Второй этап содержит отбор

заинтересованных студентов для увлекательной полноценной научно-исследовательской работы (НИР). Таким образом, НИД начинают заниматься люди творческие, с неординарным мышлением, увлекающиеся, любопытные, те студенты, которые оценивают свой интеллектуальный потенциал выше своего окружения. Поддержка студентов, вера в их способности, умение направлять их творческие задатки способствует вовлечению их в науку. Заниматься ИР совсем не значит обязательно делать открытия в науке, прежде всего необходимо глубоко изучать интересующие определённые научные направления, затем пробовать выдвигать гипотезы и проверять их научным путём, ставить и решать профессиональные задачи. Исследовательская деятельность связана с проектной деятельностью, предполагающей построение процесса в логике деятельности, имеющий личностный смысл, комплексный подход к разработке проекта, вариативность использования базовых знания и умений в реальных ситуациях [2]. Преподаватель должен владеть данной педагогической технологией, в частности, такими принципами проектной деятельности, как прогностичности, пошаговости, обратной связи. Кроме того, преподаватель должен обладать разносторонними знаниями, уметь грамотно разъяснять студентам вопросы медицинской информатики и не бояться консультироваться с медицинскими работниками по вопросам медицины, если таковые выходят за грани его знаний.

Постановка задачи

Примером исследовательской студенческой работы взят опыт кружка медицинской информатики Донецкого медицинского колледжа. *Объектом* выбрана медицинская информационно-поисковая сеть (МИПС) на базе локальной сети отделения клинической дозиметрии и радиационной безопасности Республиканского онкологического центра (РОЦ). Подготовка к проведению научного исследования включала в себя определение ведущих понятий исследовательской работы и следовала по плану:

Сформулирована постановка задачи: Исследовать обработку медицинской информации каждого звена данной МИПС. Сопоставить интеграцию информационных технологий в радиологическое отделение РОЦ с текущими технологиями и мировыми IT-трендами.

Определены исходные гипотезы:

1. Убедиться, что обработка медицинской информации на диагностических и лечебных компьютерных комплексах осуществляет циклический процесс в лечебно-диагностическом процессе.
2. Доказать интеграцию IT в лучевую терапию, как эффективное безопасное средство в лучевой терапии.

Выбрана цель работы: выявить взаимосвязь между модулями информационно-поисковой системы радиологического отделения, объединяющая диагностический и лечебный процессы, как основание циклического процесса при обработке мединформации. В работе выдержаны принципы НИД, выполнены все пункты подготовки и проведения научного исследования. Детально проведён анализ назначения, функций и взаимосвязь отдельных звеньев МИПС. Получены углубленные знания сверх учебных планов в результате практического наблюдения и изучения данной темы.

Исследование

Реализация научного исследования (аналитический, рефлективный этап) осуществлялась с предварительного изучения состава МИПС:

1) подсистемы (модуля) визуальной диагностики-КТ, МРТ;
2) подсистемы (модуля) «Система дозиметрического планирования» (СДП);
3) подсистемы (модуля) топометрических измерений – «Компьютерный симулятор»;
4) подсистемы (модуля) линейного ускорителя.

Преподавателем введены элементы проектного обучения так, чтобы от занятия к занятию подгруппы решали коллективно поставленные задачи, учитывая мнения каждого. Этапы работы над проектом, как самостоятельная и коллективная исследовательская деятельность, предполагает организации работы группами и определения роли каждого в рабочей группе [2]. Преподаватель учит наблюдать главное из всего потока информации, ставя целенаправленные задачи, учит готовить отчёты, содержащие грамотное фиксирование наблюдаемых процессов и результатов проводимого исследования в рамках научного изложения. Далее студентами последовательно проводился анализ функций и взаимосвязи отдельных звеньев локальной системы отделения. Примеры фиксированных исследований изучаемого материала носят описательный характер, что и предлагается в качестве кратких примеров, как отдельных мини-проектов.

Пример №1. Информационно-поисковая система радиологического отделения представляет собой локальную сеть, обеспечивающую хранение большого количества информации, быстрый доступ, эффективную обработку информации. Локальная сеть работает на основе технологий PACS (Picture Archiving and Communication System) - системе архивации и передачи изображений в лучевой диагностике и терапии [3]. Универсальным медицинским форматом изображений и их передачи является стандарт DICOM (Digital Imaging and Communication in Medicine – цифровые изображения и их передача в медицине) – основной стандарт, определяющий передачу и хранение медицинских диагностических изображений и сопутствующей им информации. С помощью PACS любые графические изображения подвергаются перекодировке и совместимости и становятся пригодными для сохранения в компьютерной среде, тогда как обычно в диагностических кабинетах они воспроизводятся по технологии, свойственной каждому конкретному методу.

Пример №2. Модуль «Визуальная компьютерная диагностика» состоит из медицинских приборно- компьютерных комплексов: компьютерного томографа (КТ) и магнитно-резонансного томографа (МРТ). Модуль предназначен для послойного исследования группы органов. Сбор медицинских данных происходит при помощи информационных лучей (ИЛ) – волновых процессов разной физической природы. Подсистемы визуализации (КТ, МРТ) в РОЦ выполняют функцию получения анатомо-топографических данных об опухоли и прилежащих структурах. Природа и биологическое действие информационных лучей разная: для КТ – это рентгеновские лучи, оказывающие лучевую нагрузки на пациента. Информационные лучи на МРТ - резонансное э/м излучение человека (Н –спектр). Метод безвредный ввиду отсутствия лучевой нагрузки на пациента. На данном этапе аналоговые данные реконструируются в графическое изображение. При исследовании данного вопроса можно провести междисциплинарную связь с историей медицины, указав на тот факт, что описание изображений опирается на известный Анатомический атлас распилов, который был получен Н.И. Пироговым в XIX веке из первых анатомических срезов, имеющий научную ценность в наше время (рис. 1) [4]. Для постановки диагноза эти методы являются приоритетными. При анализе полученных изображений лечащий врач принимает решение о проведении курса лучевой терапии.

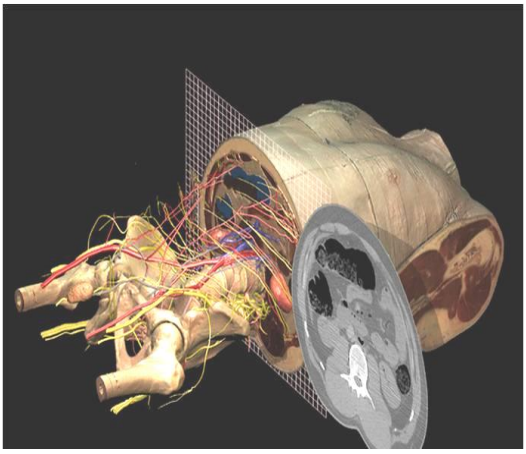


Рисунок 1 – Модель анатомического среза Н.И.Пирогова

Пример №3. Модуль «Системы дозиметрического планирования (СДП)» является первым этапом предлучевой подготовки пациента и заключается в создании модели облучаемого поля и программы управления линейным ускорителем. Цель планирования — достижение максимально равномерного дозного распределения в облучаемой мишени так, что бы здоровые прилегающие критические ткани получили минимальную лучевую нагрузку [5]. Одним из интереснейших моментов работы есть создание 3-D моделей исследуемого участка и радиационных полей (рис. 2), а так же других видов полей в виде графиков, изодозных поверхностей. Для создания моделей необходимо ввести слайсы с компьютерного томографа, оптимальную [6] дозу облучения и режим фракционирования. На основании полученных моделей можно прогнозировать лечение пациентов с большой точностью. На данном участке отмечаются профессиональная ответственность медперсонала, согласованность между медицинскими физиками и лучевыми терапевтами, обговаривающими мельчайшие детали плана облучения.

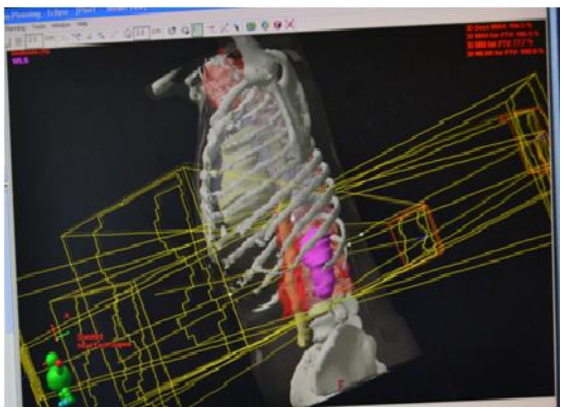


Рисунок 1 – 3-D модель облучаемого поля

Пример №4. Модуль «Компьютерная симуляция» – обязательный 2-й этап предлучевой подготовки пациента, который производится на рентгеновском симуляторе, корректирующим с предельной точностью выбранный план лечения на ускорителе. Рентгеновский компьютерный симулятор – диагностический рентгеновский аппарат, необходимый для выбора контуров (границ) радиационного поля путем геометрического моделирования пучка излучения терапевтического аппарата заданных размеров, позиции (угол наклона) и расстояния от излучателя до поверхности тела или до центра очага [7].

Пример №5. Модуль «Лучевая терапия». Линейные ускорители, используются, как один из современных методов борьбы со злокачественными образованиями всех локализаций.

В основе работы линейного ускорителя лежат микроволновые технологии. В волноводной системе линейного ускорителя происходит разгон (ускорение) электронов, которые затем сталкиваются с препятствием из тяжелого металла, что сопровождается выработкой высокоэнергетического жёсткого рентгеновского излучения. На выходе из линейного ускорителя форма полученного пучка лучей подстраивается под параметры опухолевого очага, что обеспечивает его точное облучение.

Изменение формы пучка происходит с помощью многолепесткового коллиматора, встроенного в ускоритель, или специальных блоков, которые укрепляются на аппарате извне. Наблюдается внешний вид линейного ускорителя; укладка пациента по меткам и выставленным координатам; мониторинг пациента во время лечения (рис. 3); изменение формы щели коллиматора на экране инженерного монитора.

Данный модуль знаменуется сочетанием физико-дозиметрических, технических, клинических и радиологических подходов к лечению каждого больного [8]. Программы, созданные на СДП, управляют линейным ускорителем, формируют конфигурацию высокоэнергетических потоков лучей при помощи многолепесткового коллиматора согласно конфигурации мишени.

Рисунок 2 – Наблюдение за пациентом

Пример №6. Интеграция информационных технологий в медицину ДНР в сравнении с текущими технологиями и мировыми IT-трендами. Информатизация здравоохранения в ДНР находится в стадии активного развития, тогда как в большинстве стран этот процесс вышел на уровень насыщения. Современным мировым флагманом МИПС является система iSite PACS фирмы Philips - одной из трех ведущих компаний на рынке медицинских решений. iSite PACS легко интегрируют в телемедицину, в медицину государств постсоветского пространства, в частности, Казахстана, Белоруссии, России. Мировые полноценные системы PACS оснащены алгоритмами сжатия изображений на основе вейвлет- преобразования - коэффициент сжатия до 30 раз практически без потери качества изображения (non - lossy), тогда как обычные алгоритмы не допускают коэффициентов более 4:1.

Исследовательская работа студентов, изложенная выше, представляет описательный характер. При этом показан основной ход анализа наблюдений, благодаря системе методик, помогающих последовательно понять суть поставленных задач. Эти методики представляют собой дидактические таблицы, как основные ориентиры деятельности преподавателя и студентов.

Дидактическая таблица 1. Диагностический процесс. **МРТ**

С какими МПКК знакомятся обучающиеся	Виды деятельности	Что наблюдаем	Методы	Результаты наблюдения, выводы, проблемы.
Диагностические медицинские компьютерные комплексы: МРТ	**Исследовательская деятельность**	1. Внешний вид и работу МРТ. 2. Психологическую подготовку пациента к обследованию медперсоналом. 3. Укладку пациентов в соответствии со стандартом DICOM на стол пациента в однородное магнитное поле. 4. Наложение высокочастотной резонансной катушки на обследуемый участок. 5. Включение программы сканирования. Появление изображений на мониторе. 6. Обработку медицинской информации. 7. Определение плотностей наблюдаемых структур по шкале Хаунсфилда. 8. Работу с центральной БД, архивирование и открытие графических файлов. 9. Изображения в разных режимах. 10. Описание изображений врачом.	1. **Наблюдение** диагностического процесса. 2. **Беседа** с медицинским персоналом о биологическом действия информационных лучей на МРТ. 3. **Анализ** обработки мединформации на КТ и МРТ. 4. **Обобщение** общих принципов работы на компьютерных диагностических комплексах КТ и МРТ.	1. Получение новых знаний. 2. Причины ограничения обследований на МРТ. 3. Составление схемы преобразования медицинской информации на диагностических МПКК. 4. Уровень информативности изображений на КТ и МРТ. **Формирование понятий:** • преобразование информационных лучей в графическое изображение анатомических структур. • Резонансное излучения человека (водородный спектр); • низкопольный МРТ; • сканирование; • режимы наблюдения реконструированного изображения.
	Проектное обучение	1. Фиксирование рабочего процесса малыми подгруппами.	1.Обсуждение проблемных вопросов. 2. Принцип пошагой деятельности.	1. **Составление рабочего отчёта** обработки информации (сбора, хранения, передачи) на КТ, МРТ. 2. Описание информационной поддержки диагностического процесса на визуальных компьютерных комплексах.

Дидактическая таблица 2. Лечебный процесс. СДП

С какими МПКК знакомятся обучающиеся	Виды деятельности	Что наблюдаем	Методы	Результаты наблюдения, выводы, проблемы.
МПКК предлучевой подготовки: СДП-системы дозиметрического планирования. Лечебный процесс, математическое моделирование	**Исследовательская деятельность**	1. Создание математических моделей анатомических структур на основании томограмм. 2. Просматривание моделей в разных проекциях 3. Создание графических изодозных моделей радиационных полей. 4. Создание моделей пучков лучей разных конфигураций для многолепесткового каллиматора линейного ускорителя.	1. **Наблюдение** создания математических моделей. 2. **Знакомство** со свойствами моделей. 3. **Анализ** математических моделей в лучевой терапии 4. **Осмысление** информационных процессов в предлучевой подготовке в СДП. 5. **Обобщение.** Работа СДП, как экспертная система.	1. **Получение новых знаний** о математических моделях и их роли в распределении дозной нагрузки на мишень и здоровые органы. 2. **Формирование основных понятий:** автоматизированные информационные системы, АРМ, БД, БЗ, Математические модели, дозное распределения лучевой нагрузки при помощи СДП. **Проблемы:** a) Выбор оптимального варианта поля для лечения пациента b) Распределения лучевой нагрузки по изолиниям модели поля. **Выводы:** 1. При помощи моделей радиационного поля заранее прогнозируется лечение, выбирается оптимальный вариант облучения. 2. Получены углубленные знания сверх учебных планов .
	Проектное обучение	1. Медицинские физики и лучевые терапевты моделируют объекты и процессы, согласовывая детали плана облучения.	1.Интегрирование знаний по радиологии, лучевой терапии, математике, истории медицины. 2.Принцип обратной связи.	1. Подготовка индивидуальных отчёт-проектов в рамках научного изложения. 2. Описание информационной поддержки предлучевой подготовки пациента на СДП.

Дидактическая таблица 3. Лечебный процесс. Линейный ускоритель.

С какими МПКК знакомятся обучающиеся	**Виды деятельности**	**Что наблюдаем**	**Методы**	**Результаты наблюдения, выводы, проблемы.**
Лечебный МПКК: Линейный ускоритель (лечебный процесс)	**Исследовательская деятельность**	1. Внешний вид и работу линейного ускорителя по индивидуальному плану (ПО) пациента. 2. Наблюдение автоматической работы ускорителя в разных режимах. 3. Передачу индивидуального плана пациента по сети для автоматической работы ускорителя. 4. Наблюдение сложной укладки и фиксирования частей тела для точного прицеливания лучей 5. Наблюдение на стенном мониторе ускорителя процесса совмещения координат с метками на теле пациента при помощи системы лазерных лучей. 6. В пультовой на мониторе инженера при включённом ускорителе наблюдаем формирование конфигурации луча при помощи многолепесткового коллиматора. Мониторинг пациента во время лечения.	**Синтез:** объединение модулей в единый лечебно-диагностический процесс. **Анализ** условий обработки медицинской информации в циклическом процессе. **Обобщение:** **1.** Сведение до минимума ошибок в работе каждого звена для минимизации погрешностей в едином лечебно-диагностическом процессе – залог успешного лечения.	1.**Осмысление** решения главной задачи – получение грамотного предсказуемого лечения при минимальном облучении здоровых тканей. 2.**Получение новых разносторонних знаний** на конечном этапе исследования. **Выводы:** 1. Лечение приводит к изменению параметров облучаемых областей, что заставляет их корректировать для последующего цикла. 2. 2. Интеграция IT в лучевую терапию, является высокоэффективным средством.
	Проектное обучение	Высокую культуру общения служб отделения. 1. Основные программные модули на заключительном этапе работы: ✓ модуль укладки пациента; ✓ модуль анализа данных; ✓ модуль управления ЛУ.	1. **Обсуждение** проблемных вопросов с инженерным и медицинским персоналом линейного ускорителя. 2. **Принцип прогностичности** Интегрирование знаний по лучевой терапии в сестринское дело.	1. Работа в статистическом отделе РОЦ по данным эффективности лечения на ускорителях. 2. Составление отчёт-проекта завершающего этапа информационной поддержки лечебно-диагностического процесса.

Выводы

1. Студенты убеждаются, что компьютерные технологии, интегрируемые в медицину, формируют единый лечебно-диагностический процесс.

2. Реализуется главная задача лечения – действие лучей не вызывает поражений близлежащих здоровых органов, не гибнут здоровые ткани, пациенту не угрожает инвалидность.

3. Студенты убеждаются, что гипотезы проверены научным путём на основании изучения, наблюдения, анализа.

4. Обработка различных медицинских данных и информационной поддержке производится с максимальной точностью, преобразуясь в различные виды. Так, графическая информация преобразуется в высококачественное дозноанатомическое моделирование, на основании которого создаётся специальная программа для управления ускорителем – главным инструментом в лучевой терапии.

5. Студенты чётко прослеживают условия организации циклического процесса обработки медицинской информации в лечебно-диагностическом процессе, а именно: поскольку опухоль при облучении изменяет свои размеры и форму, периодически происходит корректирование плана облучения и меток на теле пациента, т.е. повторяются вышеописанные процедуры, что составляет циклический процесс.

6. Занятия на лечебных базах несут большую эмоциональную и нравственную нагрузку. Студенты впервые сталкиваются с лечебно-диагностическим процессом онкобольных, видят отношение персонала к пациентам, учатся сопереживать, соболезновать при соприкосновении со страданием и человеческим горем.

7. Знания, приобретённые в НИР, могут быть использованы при дальнейшем изучении медицинских наук (хирургии, терапия, истории медицины и др.).

8. Появляется много новых вопросов!

Оформление отчёт–проекта исследовательской работы требует от студентов грамотного фиксирования процесса и результатов проводимого исследования в рамках научного изложения.

Проект содержит:

1) последовательное описание модулей с точки зрения системного анализа;
2) рисунки, схемы, таблицы;
3) собственные впечатления от увиденного.

Защита результатов исследования включает подготовку к публичному выступлению – не менее сложной и важной части исследовательской деятельности. Выступление с докладами на научных конференциях является обязательным итогом работы. По данному исследованию студенты научного кружка выступали на студенческих научно-практических конференциях, участвовали в конкурсах на лучшую студенческую научную работу.

Исследовательская работа студентов, как составляющая подготовки специалиста среднего звена, помогает выявлять не только творчески мыслящих студентов, она делает молодёжь интеллектуально развитой, повышают познавательную активность, тем самым увеличивает багаж знаний и умений, необходимый для формирования профессиональных компетенций. ДНР предоставляет молодёжи различные научные платформы для исследовательской работы, создаёт условия для самореализации, творческого и интеллектуального развития. Сфера применения медицинских технологий растёт, интегрируя в различные области медицины. И эта сфера расширяется с каждым днём. Сегодня быть осведомлённым в компьютеризации лечебно-диагностического процесса или даже принимать в этом участие есть неотъемлемая сторона профессиональной компетенции студентов медицинских учебных учреждений и медицинских работников [9.с.6].

Литература:

1. Тимофеева А.С., Федина В. В., Петрова Л.П.// Научно-исследовательская работа студентов в технических вузах. Сборник научных трудов. Направление 1.- Белгород, 2003. - часть 1, С.174-175

2. Колесникова И. А. Педагогическое проектирование: Учеб. пособие для высш. учеб. заведений.М: Издательский центр «Академия», 2005. — 288 с.

3. Абрамов Н.В. и др. Информационные системы в медицине: Учебное пособие— Нижневартовск: Изд-во Нижневарт. гуманит. ун-та, 2008. — 171 с. 2008. Режим доступа: [http://scicenter.online/meditsine-tehnologii-informatsionnyie/informatsionnyie-sistemyi-meditsine-uchebnoe.html

4. Шевченко Ю. Л., Китаев В. М. // Национальный медико-хирургический центр имени Н.И. Пирогова, Москва. Журнал: Хирургия. Журнал им. Н.И. Пирогова. 2010;(9): 4-8 "Ледяная анатомия" Н.И. Пирогова. Режим доступа: https://www.mediasphera.ru/journal/khirurgiya-zhurnal-im-n-i-pirogova

5. ГОСТ Р 56317-2014 Изделия медицинские электрические. Системы дозиметрического планирования. Технические требования для государственных закупок. ГОСТ Р 56317-2014

6. Линденбратен Л.Д., Королюк И.П. Медицинская радиология: Учебник. 2-е изд. М.: Медицина, 2012. -648с.

7. Абрамов Н.В. и др. Информационные системы в медицине: Учебное пособие— Нижневартовск: Изд-во Нижневарт. гуманит. ун-та, 2008. — 171 с. Режим доступа: [http://scicenter.online/meditsine-tehnologii-informatsionnyie/informatsionnyie-sistemyi-meditsine-uchebnoe.html

8. Бекман И.Н. Курс лекций Ядерная медицина. Лекция 7. Лучевая терапия. Режим доступа: http://profbeckman.narod.ru/MED7.htm

Швыдкий О. В., Момоток Л. А. Исследовательская работа студентов, как образовательная составляющая подготовки медицинского специалиста среднего звена. *В статье рассматривается исследовательская работа студентов на лечебной базе Республиканского онкологического центра (РОЦ), где использованы информационные технологии для диагностики и лечения онкологических больных. Используя элементы проектного обучения в малых подгруппах, наблюдая и анализируя исследуемые объекты, исследовательская работа, рассматривается в системе личностно-ориентированного образования и направлено как на индивидуальный поиск истины, так и коллективный. В статье воспроизведены методики последовательного ознакомления обучающихся в идее дидактических таблиц с обязательными этапами исследовательской работы, которые помогают среди потоков научной информации выбирать самое ценное для проведения системного анализа.*

Ключевые слова*: медицинская информация, медицинские приборно-компьютерные комплексы (МПКК), визуальные методы диагностики, предлучевая подготовка, системы дозиметрического планирования (СДП), топометрические процессы, рентгеновский симулятор, лучевая терапия, линейный ускоритель.*

Shvydkii O. V., Momotok L. A. Research work of students, as an educational component of the training of a medical specialist of middle level. *The article deals with research work of students on the medical base of the Republican Oncology Center (ROC), which uses information technologies for diagnosis and treatment of cancer patients. Using elements of project training in small subgroups, observing and analyzing the objects under study, research work is considered in the system of personality-oriented education and is directed both at individual search for truth and collective. The article reproduces the methods of sequential acquaintance of students in the idea of didactic tables with the obligatory stages of research that help to choose among the streams of scientific information the most valuable for carrying out system analysis.*

Keywords: *medical information, medical instrument-computer complexes, visual diagnostic methods, pre-radial preparation, dosimetry planning systems, topometric processes, X-ray simulator, radiation therapy, linear accelerator.*

Статья поступила в редакцию 18 мая 2018 г.
Рекомендована к публикации профессором Миненко А. С.

УДК 004.7

Опыт использования вузами образовательных ресурсов компании D-LINK для подготовки квалифицированных специалистов в области телекоммуникаций

П. В. Ромасевич,
доцент кафедры телекоммуникационных систем,
Волгоградский государственный университет, г. Волгоград
promasevich@dlink.ru

Ромасевич П. В. Опыт использования вузами образовательных ресурсов компании D-LINK для подготовки квалифицированных специалистов в области телекоммуникаций. *Статья посвящена рассмотрению образовательных ресурсов компании D-Link для подготовки квалифицированных специалистов для области IT, различным направлениям сотрудничества компании D-Link с высшими учебными заведениями и опыта их взаимодействия с производителем активного сетевого оборудования и использования его образовательных ресурсов в учебном процессе.*

Ключевые слова: *D-Link, IT-образование, учебные курсы, программирование, встроенные системы, Linux, направления сотрудничества IT-компаний и ВУЗов.*

Введение

В настоящее время происходит системное развитие и внедрение цифровых технологий во все области жизни: в экономику, госуправление, социальную сферу, в городское хозяйство. В связи с этим одним из важных является вопрос подготовки квалифицированных кадров для области IT.

Кафедра «Телекоммуникационных систем» создана в Волгоградском государственном университете в 2007 году [9] и является единственной в Нижнем Поволжье и на Юге России по подготовке специалистов направления 210700.62 «Инфокоммникационные технологии и системы связи». Выпускники кафедры востребованы на рынке и работают в различных сегментах экономики России и за рубежом.

Объектами профессиональной деятельности выпускников данной специальности являются широкополосные пакетные сети передачи данных, сети Интернет вещей, автоматические телефонные станции, системы сотовой связи, системы цифровой телефонии и многоканальной передачи, IP-телефония и Internet технологии, сети PDH\SDH, волоконно-оптические системы и линии связи.

Смена телекоммуникационных технологий происходит быстрее, чем образовательная система успевает адаптироваться к изменениям. В результате выпускники зачастую имеют хорошую теоретическую базу, но не умеют решать реальные задачи и нуждаются в длительной адаптации на производстве.

В этой связи важную роль в процессе IT-образования играют программы обучения производителей телекоммуникационного оборудования. Поэтому уже более 10 лет компания D-Link развивает собственную программу обучения, направленную на подготовку квалифицированных специалистов [1].

С момента образования в 2006 году регионального офиса D-Link по Волгоградской, Астраханской областям и республике Калмыкия кафедра «Телекоммуникационных систем» активно взаимодействует с вендором в Волгограде.

По инициативе автора, который также является руководителем регионального офиса, на кафедре «Телекоммуникационных систем» Волгоградского государственного университета уже несколько лет успешно функционирует лаборатория «Мультсервисных систем и сетей» для проведения научных исследований и учебного процесса в области широкополосных пакетных сетей передачи данных. Так, на базе лаборатории автор читает лекции для бакалавров и магистров по курсам «Сети связи», «Современные цифровые системы передачи», «Мультисервсиные сети» и проводит лабораторные практикумы с использованием образовательных ресурсов D-Link в рамках учебного плана кафедры.

Активное взаимодействие регионального офиса D-Link с профильной кафедрой также включает в себя научные исследования, руководство научно-исследовательскими и дипломными работами бакалавров и магистрантов, ежегодную работу в ГЭК и ГАК и участие в организации ежегодной Всероссийской конференции «Проблемы передачи информации в телекоммуникационных системах»,

индексируемой в Российском индексе научного цитирования (РИНЦ).

Обзор учебных курсов D-Link

Условно процесс обучения по программам компании D-Link можно разделить на две составляющие: фундаментальные знания в области информационных технологий и конкретные навыки работы с продуктами, предлагаемыми на рынок.

В настоящее время для изучения в очной форме, а также на портале дистанционного обучения и сертификации D-Link доступны следующие учебные курсы (рис.1):

- «Основы сетевых технологий. Часть 1: Основы передачи и коммутации данных в компьютерных сетях»;
- «Основы сетевых технологий. Часть 2: Основы беспроводных сетей Wi-Fi»;
- «Технологии коммутации и маршрутизации современных сетей Ethernet. Базовый курс D-Link»;
- «Основы сетевой безопасности. Часть 1: Межсетевые экраны»;
- «Основы сетевой безопасности. Часть 2: Технологии туннелирования»;
- «Использование Linux при программировании».

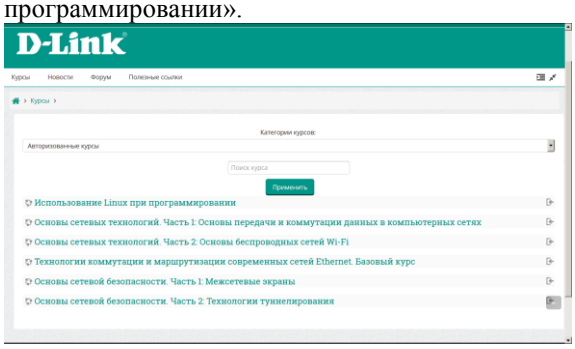


Рисунок 1 – Учебные курсы D-Link

Курс «Основы сетевых технологий. Часть 1: Основы передачи и коммутации данных в компьютерных сетях» является вводным и служит для получения базовых знаний о сетевых технологиях. В нем подробно рассматриваются технологии физического и канального уровней модели OSI, механизмы сетевого взаимодействия, принципы проектирования компьютерных сетей. Помимо протокола IPv4, в курсе рассматривается протокол IPv6. Курс знакомит с такими сетевыми устройствами, как точки доступа, коммутаторы, маршрутизаторы и методами их настройки и управления.

Поддержку теоретической части обеспечивают лабораторные работы, которые учат создавать простую коммутируемую сеть, начиная от обжимки кабелей и заканчивая настройкой коммутаторов, соединяющих клиентские устройства. По курсу предусмотрен сертификационный экзамен.

Курс «Технологии коммутации и маршрутизации современных сетей Ethernet. Базовый курс D-Link» посвящен рассмотрению технологий уровня доступа и распределения компьютерных сетей. Он учит созданию коммутируемых и маршрутизируемых локальных сетей, удовлетворяющих требованиям «Triple play» по передаче голоса, видео и данных на базе оборудования D-Link. Этот курс позволяет получить знания по сегментации сетей, повышению надежности и производительности, обеспечению качества обслуживания (QoS). Большое место в курсе уделено обеспечению безопасного доступа в сеть. Рассматриваются такие функции как ACL (Access Control List), Port Security, IP-MAC-Port Binding, аутентификация 802.1X, Safeguard Engine, Traffic Mirroring, защита протоколов семейства STP. Эти функции, наряду с другими, позволяют защищать сеть от преднамеренных и непреднамеренных угроз.

В курсе предусмотрены 24 лабораторные работы, охватывающие все рассмотренные в теоретической части темы. По курсу можно сдать сертификационный экзамен.

Следует отметить, что совместно с преподавателями МГТУ им. Н.Э. Баумана курс издан в виде учебного пособия «Технологии коммутации и маршрутизации в локальных компьютерных сетях», имеющего гриф УМО для направления «Информатика и вычислительная техника» [2].

Курс «Основы сетевых технологий. Часть 2: Основы беспроводных сетей Wi-Fi» появился в конце 2016 года. Данный курс позволяет получить знания по проектированию и развертыванию беспроводных сетей малых и средних предприятий, корпоративных сетей, а также об их интеграции с проводными сетями. Показано поэтапное проектирование беспроводных сетей – от планирования производительности и зоны действия, до развертывания сети. Приведены подробные методики и примеры расчета производительности и зоны действия. Показана работа с инструментом Wi-Fi Planner Pro, разработанным D-Link (рис.2).

Рисунок 2 – Инструмент Wi-Fi Planner Pro

Отличительной особенностью курса является подробное рассмотрение спецификаций физического уровня 802.11n и 802.11ac. Подробно описаны такие функции как формирование диаграммы направленности передатчика, механизмы защиты при работе в сети устройств разных спецификаций 802.11, механизмы сосуществования при использовании каналов разной ширины, описание которых, как правило, отсутствует в русскоязычной литературе, посвященной теме Wi-Fi. При рассмотрении спецификации 802.11ac описана технология MU-MIMO, механизм работы с динамической полосой пропускания при использовании в сети каналов шириной 80 МГц, 160 МГц, 80+80 МГц. Эти функции еще только начинают внедряться в оборудование разных производителей, выходящее на рынок. Также в курсе подробно рассмотрено подключение клиента к сети в инфраструктурном режиме – сканирование, методы аутентификации и ассоциации, вопросы безопасности передачи данных в беспроводных сетях (WEP, TKIP, CCMP, WPA/WPA2, WPS). Не остались без внимания вопросы организации роуминга на 2 и 3 уровне модели OSI, описана технология интеллектуального распределения клиентов, разработанная D-Link. В курсе показана работа с такими средствами поиска неисправностей как InSSIDer, Microsoft Network Monitor. Рассматриваются особенности использования радиочастотного спектра в Российской Федерации. Помимо этого в курсе показано применение комплексного решения D-Link для организации беспроводных сетей, в основе которого лежит использование беспроводных контроллеров.

В курсе «Основы сетевых технологий. Часть 2: Основы беспроводных сетей Wi-Fi» имеется 13 лабораторных работ, поддерживающих темы, рассматриваемые в теоретической части.

Совместно с преподавателями МГТУ им. Н.Э. Баумана курс издан в виде учебного пособия «Технологии современных беспроводных сетей Wi-Fi» для студентов (адъюнктов), обучающихся по основным образовательным программам высшего образования по направлениям подготовки бакалавриата/магистратуры укрупненной группы специальностей и направлений подготовки 09.00.00 «Информатика и вычислительная техника» [3].

Вопросы безопасности компьютерных сетей и решения компании D-Link в этом направлении отражены в курсах «Основы сетевой безопасности. Часть 1. Межсетевые экраны» и «Основы сетевой безопасности. Часть 2. Технологии туннелирования», которые являются совместной рабой с преподавателями МГУ им. М. В. Ломоносова. В курсе «Основы сетевой безопасности. Часть 1. Межсетевые экраны» внимание уделяется изучению основных принципов создания надежной и безопасной ИТ-инфраструктуры, способам сегментирования сетей на канальном уровне, классификации межсетевых экранов и созданию политик межсетевых экранов. Рассмотрены основные технологии и способы классификации систем обнаружения и предотвращения проникновений, способы приоритезации трафика и создания альтернативных маршрутов. Большое внимание уделено практическим вопросам. Теория поддерживается 12 лабораторными работами на межсетевых экранах D-Link.

В курсе «Основы сетевой безопасности. Часть 2. Технологии туннелирования» основное внимание уделяется изучению наиболее важных сервисов и механизмов защиты информации в сети Интернет, а именно, криптографических алгоритмов и протоколов, в которых используются эти алгоритмы. Большое внимание уделено практическим вопросам. Теория поддерживается 14 лабораторными работами на межсетевых экранах D-Link.

Оба курса изданы в виде одноименных книг, которые имеют гриф УМО для направлений «Прикладная математика и информатика» и «Фундаментальная информатика и информационные технологии» [4].

С каждым годом растет интерес к профессии программиста, но далеко не все представляют, что нужно знать и уметь, чтобы стать высококвалифицированным специалистом в области программирования. Центр исследований и разработки, расположенный в Рязани, столкнулся с проблемой отсутствия необходимых знаний для программирования сетевых устройств у выпускников учебных заведений. Во-первых, на выработку практических навыков программирования в рамках учебных программ ВУЗов и СУЗов отведено небольшое количество часов, во-вторых, у выпускников зачастую отсутствуют навыки инженерного мышления и понимание тех задач, которые решаются при промышленном программировании.

Подготовка квалифицированного программиста для разработки программного обеспечения сетевых устройств базируется на следующих дисциплинах телекоммуникационных специальностей: «Физика», «Операционные системы», «Микроконтроллеры» или «Программирование микроконтроллеров». Зачастую в рамках специальности эти дисциплины читаются как самостоятельные курсы, несмотря на то, что они тесно связаны при решении различных задач по разработке программных средств.

Большинство производимых и разрабатываемых компанией D-Link сетевых устройств представляют собой, по сути, специализированные компьютеры (встроенные системы), функционирующие под управлением операционной системы Linux. На базе Рязанского государственного радиотехнического университета компанией D-Link организованы факультативные занятия для студентов по тематике разработки программного обеспечения встроенных систем на основе Linux. В рамках этих занятий изучаются основы работы с командным интерфейсом Linux, основы программирования на языке C, устройство ядра Linux, работа с программными интерфейсами ядра Linux, основы использования Linux и свободных программ во встроенных системах. На основе первой части материалов данных факультативных занятий разработан дистанционных курс «Использование Linux при программировании». Целью данного курса являются приобретение знаний и навыков работы с операционной системой Linux на уровне пользователя, а также навыков использования ряда утилит Linux для решения типовых задач, стоящих перед программистом. При выполнении лабораторной части курса студенты осваивают открытый инструментарий программиста для Linux – компилятор GCC, систему сборки Make, отладчики GDB и DDD, систему контроля версий Git. Планируется разработка и других дистанционных курсов в области Linux-программирования на основе пока не использованных материалов факультативных занятий в РГРТУ.

Программное обеспечение встроенных систем должно работать в условиях сильно ограниченных ресурсов. Встроенные системы могут применяться в разных сферах: от систем контроля за спутниками до высокочастотного алгоритмического трейдинга. Они отличаются аппаратной частью, операционными системами, стилями программирования. Тем не менее, у них существуют определенная схожесть.

Для обучения системному подходу к программированию встроенных систем, компания D-Link ведет разработку учебного курса, объединяющего в себе изучение методов программирования, операционных систем, аппаратного обеспечения оборудования и сетевых технологий. Курс будет содержать теоретическую часть и лабораторный практикум на базе микроконтроллеров.

Виды сотрудничества с D-Link

В рамках программы обучения существует несколько направлений сотрудничества D-Link с учебными заведениями. Учебное заведение может:

- открыть авторизованный учебный центр D-Link и обучать в нем всех заинтересованных лиц;
- стать академическим партнером D-Link и использовать учебные материалы D-Link или разрабатывать на их основе собственные в рамках учебных программ высшего, среднего, специального образования;
- проводить обучение в дистанционной форме, используя уже готовые курсы дистанционного обучения D-Link, либо разработать совместно с представителями компании собственные курсы;
- открыть учебные классы D-Link и обучать в них по разработанным преподавателями учебного заведения авторским курсам D-Link;
- открыть сетевую лабораторию D-Link для поддержки практических занятий, курсов дистанционного обучения и исследовательской деятельности.

Вне зависимости от формы сотрудничества компания D-Link предоставляет учебному заведению возможность бесплатного обучения преподавателей, получения учебных материалов, консультаций специалистов, доступ к технической документации на оборудование. Помимо этого, с целью поддержки учебного процесса в рамках академического партнерства, возможно предоставление оборудования для проведения лабораторных работ согласно учебной программе.

Учебные материалы доступны для самостоятельного изучения на портале дистанционного обучения D-Link [5]. С момента открытия портала в 2011 году, обучение на нем прошли более 20 000 человек. Более 2 000 человек сдали сертификационные экзамены.

С целью разработки учебных пособий по различным сетевым технологиям компания активно сотрудничает с преподавателями ведущих ВУЗов страны. Так совместно с преподавателями МГТУ им. Н.Э. Баумана изданы учебные пособия «Построение коммутируемых компьютерных сетей», «Технологии защиты информации в компьютерных сетях. Межсетевые экраны и интернет-маршрутизаторы», «Технологии коммутации и маршрутизации в локальных компьютерных сетях», «Технологии современных беспроводных сетей Wi-Fi» с грифом УМО для направления «Информатика и вычислительная техника».

Совместно с преподавателями МГУ им. М. В. Ломоносова изданы учебные пособия «Основы сетевой безопасности. Часть 1. Межсетевые экраны» и «Основы сетевой безопасности. Часть 2. Технологии туннелирования», которые имеют гриф УМО для направлений «Прикладная математика и

информатика» и «Фундаментальная информатика и информационные технологии».

Разработанные в России учебные пособия были переведены на английский язык и изданы за рубежом для поддержки международной программы обучения D-Link Academy.

В настоящее время на территории России действуют более 20 авторизованных учебных центров [6]. Более 50 российских учебных заведений высшего и среднего образования стали академическими партнерами D-Link [7].

Академическим партнером D-Link может стать любое образовательное учреждение, заинтересованное в развитии системы IT-образования и внедрении в образовательный процесс информации о новейших сетевых технологиях и практических примерах их использования, а также в повышении квалификации преподавателей. Для приобретения практических навыков работы с сетевым оборудованием D-Link способствует организации производственной практики студентов ВУЗов и СУЗов на базе региональных офисов и созданию в учебных заведениях лабораторий сетевых технологий, в которых студенты и преподаватели могут вести также исследовательскую работу в области телекоммуникаций.

Пример интеграции D-Link и высшего учебного заведения

Особое место среди офисов D-Link в России занимает Рязанский офис, который был открыт в 2005 г. С 2007 года в нем располагается центр разработки и исследований, который выполняет разработку внутреннего программного обеспечения для маршрутизаторов, точек доступа и других устройств, а также адаптацию встроенного программного обеспечения под нужды конкретных корпоративных заказчиков на отечественном рынке [8].

Отдельно необходимо сказать об опыте комплексного взаимодействия компании D-Link с Рязанским государственным радиотехническим университетом (РГРТУ) на различных этапах учебного процесса, создания авторизованной лаборатории, производственной практики и последующего трудоустройства студентов в компанию.

Ряд учебных дисциплин факультета вычислительной техники РГРТУ построены на основе учебных и учебно-методических разработок специалистов компании D-Link по темам: «Основы сетевых технологий», «Основы построения беспроводных сетей», «Технологии коммутации компьютерных сетей». К проведению учебного процесса активно привлекаются консультанты компании D-Link, специализирующиеся на определенном типе сетевого оборудования. Они проводят учебные семинары, включающие теоретическую часть и примеры построения реальных корпоративных сетей.

На базе кафедры ЭВМ РГРТУ действует авторизованная сетевая лаборатория D-Link. В ней проводятся практические занятия со студентами по различным дисциплинам, связанным с сетевыми технологиями, а также учебные занятия и исследовательская работа студентов в области встроенных систем на базе операционной системы Linux.

В учебные программы магистратуры по направлению «Конструирование и технология электронных средств» включена дисциплина «Встроенные компьютерные системы». Магистранты, обучающиеся по данному направлению, изучают устройство и методы разработки встроенных систем на основе операционной системы Linux на примере сетевого оборудования компании D-Link.

На базе рязанского офиса и лаборатории сетевых технологий D-Link в РГРТУ каждый год проходят производственную практику порядка 40 студентов специальностей «Математическое обеспечение и администрирование информационных систем», «Вычислительные машины, комплексы, системы и сети», «Программное обеспечение вычислительной техники и автоматизированных систем» и направлений «Информатика и вычислительная техника», «Информационные системы и технологии» и «Программная инженерия». Практика проводится по двум направлениям – «Компьютерные сети» и «Программирование».

Первое направление предполагает углубленное изучение сетевых технологий и проектирования компьютерных сетей. Второе направление предполагает разработку различных компонентов встроенного программного обеспечения сетевого оборудования D-Link, которая производится под руководством ведущих программистов компании.

Студенты, хорошо показавшие себя на практике, приглашаются на работу в отдел технической поддержки и отдел программирования компании.

О компании D-Link

Компания D-Link является ведущим мировым производителем сетевого оборудования, предлагающим широкий набор решений для создания локальных сетей Ethernet/ Fast Ethernet/ Gigabit Ethernet, построения беспроводных сетей и организации широкополосного доступа, передачи изображений и голоса по IP (VoIP). В 2012 году компания открыла в Российской Федерации собственное производство, сертифицированное в соответствии с требованиями ГОСТ Р ИСО 9001-

2008 (ISO 9001:2008). В РФ офисы компании D-Link открыты в Москве, Санкт-Петербурге, Архангельске, Волгограде, Воронеже, Екатеринбурге, Иркутске, Казани, Калининграде, Кемерово, Краснодаре, Красноярске, Курске, Н.Новгороде, Новосибирске, Омске, Перми, Ростове-на-Дону, Рязани, Самаре, Саратове, Таганроге, Туле, Тюмени, Уфе, Хабаровске, Челябинске и Ярославле. В Брянске работает региональный представитель компании.

Авторизованные учебные центры работают в Москве, Санкт-Петербурге, Абакане, Екатеринбурге, Ижевске, Иркутске, Красноярске, Магнитогорске, Новокузнецке, Новосибирске, Омске, Перми, Приволжском федеральном округе, Ростове-на-Дону, Рязани, Ставрополе, Челябинске и Ярославле. Портал дистанционного обучения D-Link: http://learn.dlink.ru. Информация о продуктах, решениях, событиях и текущей деятельности D-Link публикуется на официальном сайте http://www.dlink.ru и странице компании в Facebook.

Выводы

Опыт продвижения учебных программ D-Link в систему высшего образования для подготовки специалистов разного уровня в области информационных технологий оказался достаточно успешным, как для самой компании, так и для вузов-партнеров. При этом студенты имеют возможность подтвердить качество своих знаний не только государственным дипломом об образовании, но и сертификатами от компании D-Link по отдельным профильным дисциплинам.

Литература

1. Портал Dlink.ru [Электронный ресурс]. – Режим доступа: http://www.dlink.ru/up//docs/Learn/ Education_Program_D-Link_v.7.pdf
2. Портал Dlink.ru [Электронный ресурс]. – Режим доступа: http://www.dlink.ru/up//docs/book/ Routing_ and_switching_technology_in_LAN.pdf
3. Портал Dlink.ru [Электронный ресурс]. – Режим доступа: http://www.dlink.ru/up/ support/Learn/2016/WI-Fi_Technology_content.pdf
4. Портал Dlink.ru [Электронный ресурс]. – Режим доступа: http://www.dlink.ru/ru/education/6/
5. Портал Dlink.ru [Электронный ресурс]. – Режим доступа: http://learn.dlink.ru/login/index.php
6. Портал Dlink.ru [Электронный ресурс]. – Режим доступа: http://www.dlink.ru/ru/education/2/
7. Портал Dlink.ru [Электронный ресурс]. – Режим доступа: http://www.dlink.ru/ru/education /art/5/26.html
8. Портал Dlink.ru [Электронный ресурс]. – Режим доступа: http://www.dlink.ru/ru/about/
9. Портал Volsu [Электронный ресурс]. – Режим доступа: http://www.volsu.ru/struct/ institutes/ ipt/telecommunication/

Ромасевич П. В. Опыт использования вузами образовательных ресурсов компании D-LINK для подготовки квалифицированных специалистов в области телекоммуникаций. *Статья посвящена рассмотрению образовательных ресурсов компании D-Link для подготовки квалифицированных специалистов для области IT, различным направлениям сотрудничества компании D-Link с высшими учебными заведениями и опыта их взаимодействия с производителем активного сетевого оборудования и использования его образовательных ресурсов в учебном процессе.*

Ключевые слова*: D-Link, IT-образование, учебные курсы, программирование, встроенные системы, Linux, направления сотрудничества IT-компаний и ВУЗов.*

Romasevic P. V. Experience in the use of educational resources D-LINK for the training of qualified specialists in the area of telecommunications. *Article is devoted to consideration of D-Link company educational resources for training qualified specialists for the IT area, to various directions of cooperation D-Link company with higher educational institutions and their experience of interaction with the producer of the fissile network equipment and use its educational resources in educational process.*

Keywords*: D-Link, IT education, training courses, programming, embedded systems, Linux, directions of cooperation IT-companies and universities.*

Статья поступила в редакцию 27апреля 2018 г.
Рекомендована к публикации доцентом Зори С. А.

CONTENT

Computer and information science

Computer science and engineering

Engineering education

Электронное периодическое издание

Научный журнал

ИНФОРМАТИКА И КИБЕРНЕТИКА

(на русском, английском языках)

№ 2 (12)-2018

Ответственный за выпуск А. И. Андрюхин

Технический редактор Р. В. Мальчева

Компьютерная верстка А. И. Воронова

Подписано к выпуску 22.06.2018. Усл. печ. лист. 12. Уч.- изд. лист. 7,9.

Адрес редакции:ДНР, 83001, г. Донецк, ул. Артема, 58, ГОУ ВПО «ДонНТУ»,
5-й учебный корпус, к. 425. Тел.: +38 (062) 301-08-56 E-mail: infcyb.donntu@yandex.ru,
URL: http://infcyb.donntu.org