CENTRAL ASIAN JOURNAL OF MATHEMATICAL THEORY AND COMPUTER SCIENCES
http://cajmtcs.centralasianstudies.org/index.php/CAJMTCS
Volume: 02 Issue: 11 | Nov 2021 ISSN: 2660-5309

# Исследования вопросов критериев криптостойкости алгоритмов непрерывного шифрования

**Д. Е. Акбаров[1], О. Э. Кушматов[2], Ш.А. Умаров[3], А.Орипов[4]**

[1]*д. физ.-мат. н., Какандский государственный педагогический институт, Каканд, Узбекистан*

[2]*к. физ.-мат. н., Ферганский филиал Ташкентского университета информационных технологий, Фергана, Узбекистан*

[3]*Исследователь, Ферганский филиал Ташкентского университета информационных технологий, Фергана, Узбекистан*

[4]*старший преп, Ферганский политехнический институ, Фергана, Узбекистан*

**Аннотация:**

В статье исследованы особенности критериев стойкости алгоритмов непрерывного шифрования. Выявлены общие свойства моделей алгоритмов класса непрерывного шифрования. На их основе сформулированы соответствующие требования в виде критериев, определяющих необходимые условия криптостойкости. Совокупность этих критериев сформулировано как утверждение.

**ARTICLEINFO**

***Article history:***
Received 30 Sep 2021
Revised form 22 Oct 2021
Accepted 17 Nov 2021

**Ключевые слова:** классы алгоритмов шифрования, идеально стойкий алгоритм, непрерывный алгоритм шифрования, критерий, криптостойкость, необходимое условие, математическая модель, преобразование распространения, преобразование перемешивания, коллизия, длина ключа, шифр обозначение, шифр величина, открытое сообщение, шифрованное сообщение, микропроцессор, нелинейность, односторонность, равновесие, регулярность, лавинный эффект, гибкость преобразования относительно модификации, корреляция и коллизия.

---

**Введение.** Идеально стойкие алгоритмы шифрования являются надежными при криптографической защите информации. Тем не менее, при использовании в практических приложенях, возникают некоторые неудобства. В частности, длина ключевого блока имеет последовательность символов большого объема. Из-за этого свойства, например, могут возникать проблемы хранения и передачи ключей.

**Постановка задачи.** Исследования на пути устранений неудобств, вследствие большого объема длины ключа, естественным образом привело к задаче необходимости разработки алгоритма шифрования более удобного, с сохранением основных свойств идеально стойкого алгоритма шифрования. В предлагаемой статье формулируется необходимые условия стойкости алгоритмов непрерывного шифрования в виде утверждения.

**Решение задачи.** Известно, что поставленная задача решена на основе генераторов, вырабатывающих псевдослучайные последовательности. Генераторы псевдослучайных последовательностей по исходному ключу с длиной не меньше 256 символов, на базе односторонных (необратимых) преобразований, как: независимо преобразующих битов, полубайтов и байтов, таблицы сжатия, матричных расширений с пропорциональными строками и столбцами, логических операций и табличной замены с равномерным распределением элементов в таблице истинности, комбинацией моделей генераторов псевдослучайных последовательностей и т.д. [1-`14].

С исходным ключом относительно малой длины, но в настоящее время не меньше 256 символов, с генератором псевдослучайной последовательности, на основе односторонних преобразований, вырабатывается последовательность достаточно большой длины, элементы которой с некоторой операцией преобразуются (гаммируются) с символами шифруемого сообщения. Таким образом, разрабатывается алгоритм непрерывного шифрования.

Проведенные системные исследования и научные наблюдения авторов, позволили сформулировать следующее утверждение как необходимые условия для критериев оценки стойкости алгоритмов непрерывного шифрования

**Утверждение.** *Для того чтобы алгоритм непрерывного шифрования был криптостойким необходимо выполнение следующих условий:*

1) *Алгоритм должен быть открытым, его криптостойкость зависит не только от неизвестности ключа, еще от длины ключа, он должна быть не меньше 256 битов:* $k = k_1 k_2 ... k_N, \quad k_i \in \{0;1\}, N = 32 \times l, \quad l = 8,9, \ldots < \infty$;

2) *Операции применяемые в преобразованиях алгоритма должны соответствовать эффективному использованию в микропроцессорах, микроконтроллерах и компьютерных вычислительных системах ;*

3) *Обеспечены свойства эффективного перемешивания и распространения оснавных базовых преобразований: нелинейности, односторонности, равновесия, регулярности, лавинного эффекта, гибкости относительно корреляции и т.д.;*

4) *Алгоритм должен обеспечить выработку достаточно большой длины периода псевдослучайной последовательности на основе исходного ключа при осуществлении процесса шифрования;*

5) *Выработанные блоки псевдослучайной последовательности должны обладать свойством равномерного распределения по битам, двум битам и т.д.;*

6) *Все гамма элементы (биты, полубайты, байты и дугие подблоки) псевдослучайной последовательности должны получаться под влиянием других элементов (как псевдослучайной последовательности вырабатываемых на основе регистров сдвига), т.е. осуществляться эффективное перемешивание*;

7) *Гамма элементы (биты, полубайты, байты и другие под блоки) псевдослучайной последовательности должны обладать свойствами достаточно высокой случайности.*

**Доказательство.** Если алгоритм непрерывного шифрования криптографически стойкий, то выполняются условия, приведенные в утверждении. Необходимые криптографические характеристики этих условий обосновываются тем, что их невыполнение могут быть основой, отрицательно влияющие на стойкость алгоритма. Ниже обосновываются криптографические особенности условий, приведенных в утверждении.

**1.** Требование первого условия обеспечивает, чтобы не было сомнения в стойкости алгоритма шифрования со стороны пользователей разного рода, тем самым соблюдается общепринятый принцип Кирхгофса.

Символы ключа определяются на основе принципа использования в преобразованиях алгоритма шифрования. При этом длина исходного ключа, в настоящее время, должна быть не меньше 256 символов:

а) если преобразования осуществляются над битами, то длина исходного ключа не меньше 256 битов;

б) если преобразования осуществляются над полубайтами или байтами, то длина исходного ключа не меньше 256 полубайтов или байтов соответственно.

**2.** Второе требование, алгоритмы непрерывного шифрования должны содержать преобразования, не сложных вычисляемых операций, позволяющих широко и удобно реализовать их в аппаратных средствах [1-16].

В противном случае, т.е. неэффективность операций преобразований алгоритма шифрования в приложениях микропроцессоров, микроконтроллеров, компьютеров и других вычислительных устройств информационной технологии, ограничит их широкое применение. Приложения операции табличной замены, с таблицей истинности при равномерно распределенных элементах, является целесообразным.

**3.** Третье требование необходимо для того, чтобы обеспечить стойкость преобразования алгоритма к криптографическим атакам. Если базовые преобразования осуществляются операциями над битами или их объединениями, то без обеспечения эффективного перемешивания и рассевания могут быть основой моделирования способов крипто атак разного рода, исходя из результатов статистического анализа:

а) Свойства эффективного перемешивания и рассейивания преобразований при входных блоках $\left(x_1^i, x_2^i, \ldots, x_n^i\right),\ i = 0,\ldots,2^{n-1}$ и выходных блоках, где $n \geq m$, проверяются и вследствие определяются равномерным распределением выходных блоков в их таблице истинностей;

б) Независимость совокупность выходных блоков относительно совокупности входных блоков – свойство псевдослучайности обеспечит нелинейность преобразования.

Выполнение условия а) обеспечит свойства преобразований, как: равновесие, регулярность, лавинный эффект, корреляционная иммунность и др.

**4.** Четвертое требование обеспечит свойства стойкости преобразований относительно атак с использованием обратных преобразований алгоритма. В частности, ограничит криптографическую атаку: зная некоторую часть криптограмм, можно найти исходный ключ генератора – алгоритма псевдослучайной последовательности.

Если базовые преобразования генератора и алгоритма не имеют односторонних преобразований, то пользуясь обратными преобразованиями можно моделировать средства, криптографической атаки для раскрытия нужной информации.

С теоретической точки зрения можно составить таблицу истинности любого преобразования, исходя из возможных входных блоков и соответствующих выходных блоков, на основе многочленов Жегалкина [14-23]. Но свойства многозначной замены базовых преобразований непрерывного шифрования, с практической точки зрения, усложняют моделирования обратных преобразований.

**5.** Пятое требование обеспечивает, чтобы длина ключа гаммирования была достаточной длины. Вследствие достигается, что мощность совокупности символов в таблице шифробозначиний будет достаточна большая и обеспечится эффективное осуществление шифрования многозначной замены.

Случай, когда алгоритм не генерирует псевдослучайную последовательность достаточно большой длины, является основой не эффективного осуществления многозначной замены в процессе шифрования. Проверка периода длины псевдослучайной последовательности $c_1c_2c_3c_4 \dots c_8c_9 \dots$ осуществляется следующим образом: блок элементов псевдослучайной последовательности до некоторого номера $i = N$, $i = 2,3,\dots, N < \infty$, т.е. блок $c_1c_2 \dots c_N$ тождественно не повторяется следующим блоком $c_{N+1}c_{N+2} \dots c_{2N}$. Нижняя грань значения $N$ определяет период длины ключа [24-29].

**6.** Шестое требование обеспечит стойкость выработанной псевдослучайной последовательности как ключ гаммирования с некоторой операцией, символов шифруемого сообщения с символами псевдослучайной последовательности.

В блоке, выработанной псевдослучайной последовательности с генератором алгоритма непрерывного шифрования, его подблоки: с одним, двумя, тремя и т.д. элементами, должны повторяться случайным образом. Такая особенность проверяется статистическими тестами случайности, например, «Хи-квадрат» критерием.

**7.** Седьмое требование обеспечит, чтобы подблоки псевдослучайной последовательности были достаточной степени случайными.

Если элементы (с одним, двумя. тремя. полубайтами и т.д.) не образуются с участием других частей, то части выработанной псевдослучайной последовательности не обладают свойствами достаточной случайности.

Использование «Хи-квадрат» критерия, для определения степени случайности распределения элементов и объединений элементов в составе псевдослучайной последовательности, осуществляется следующим образом.

Результаты некоторого процесса пусть будут в количестве k: $y_1, y_2, \dots, y_k$, и этот процесс независимо произведен $n$ раз. При этом $n$ в несколько достаточное число раз кратно больше относительно числа $k$, то есть $n > k$. При этом решается задача: повторение результатов $y_1, y_2, \dots, y_k$ насколько отклоняются от равномерного $Y_1 = Y_2 = \dots = Y_k$ повторения, где $Y_s, s = 1,\dots,k;$ означают количество повторения результатов $y_1, y_2, \dots, y_k$, соответственно при независимом произведении процесса достаточно много раз $n$, относительно количества результатов $k$.

Для этого вводятся следующие обозначения:

$p_s$ –вероятность того, что результат процесса будет $y_s$, где $s = 1,2,\dots,k$;

$Y_s$ – количество результатов процесса $y_s$, при проведения процесса независимо $n$ раз.

По этим обозначениям, формула так называемого критерия «Хи-квадрат», выражающего среднеквадратичное отклонение результатов некоторого процесса от равномерного распределения его результатов выгладит:

$$V = \sum_{s=1}^{k} \frac{(Y_s - np_s)^2}{np_s}.$$

Если наблюдаемый процесс независимым образом произведен достаточно много раз и при этом рзультаты процесса $y_1, y_2,..., y_k$ всегда повторяются одинаковом количестве, т.е. $Y_1 = Y_2 = ... = Y_k$ , то имеют место соотношения $p_1 = p_2 = ... = p_k = \frac{1}{k}$ , следовательно справедливы равенства

$$V = \sum_{s=1}^{k} \frac{\left(Y_s - \frac{n}{k}\right)^2}{\frac{n}{k}} = \sum_{s=1}^{k} \frac{\left(\frac{n}{k} - \frac{n}{k}\right)^2}{\frac{n}{k}} = 0 .$$

Но, в большинстве реальных практических случаях, такое обстоятельство не наблюдается. Пусть при независимом проведении процесса в достаточном большом количестве $n$ раз, вероятность того, что результаты процесса $y_1, y_2,..., y_k$ равны, т.е. $p_1 = p_2 = ... = p_k = \frac{1}{k}$, кроме того значения количества повторений $Y_1, Y_2,..., Y_k$ не являются равными между собой. Тогда, следующая формула

$$V = \sum_{s=1}^{k} \frac{\left(Y_s - \frac{n}{k}\right)^2}{\frac{n}{k}} = \frac{k}{n} \sum_{s=1}^{k} \left(Y_s - \frac{n}{k}\right)^2$$

выражает среднеквадратичное отклонение от равномерного распределения $Y_1 = Y_2 = ... = Y_k = \frac{n}{k}$, неравномерное распределение $Y_1, Y_2,..., Y_k$ . В этой последней формуле выражение $\left(Y_s - \frac{n}{k}\right)$ ограничено некоторой константой, т.е. $\left|Y_s - \frac{n}{k}\right| \le C = const$ . Поэтому, имея адекватную модель течения процесса, можно осуществить следующее. Соответствующим образом: определяя значения его параметров, автоматизируя нужные вычисления программными средствами, проведя в большом количестве (т.е. $n \to \infty$), независимые процессы по генерации элементов псевдослучайной последовательности, получим соотношение:

$$V = \sum_{s=1}^{k} \frac{\left(Y_s - \frac{n}{k}\right)^2}{\frac{n}{k}} = \frac{k}{n} \sum_{s=1}^{k} \left(Y_s - \frac{n}{k}\right)^2 \le \frac{k}{n} \sum_{s=1}^{k} C^2 = \frac{(kC)^2}{n} \to 0 .$$

Это значит, если проведено достаточно большое количество независимых процессов по генерации элементов псевдослучайной последовательности и при этом биты, полубайты, байты и другие части, в блоке последовательности распределены почти равномерно, то значение критерия «Хи-квадрат» распределения стремится к нулю. Следовательно, делается заключение, что степень случайности выработанной псевдослучайной последовательности достаточно высокое [32-41].

Вышеприведённые математические модели легко модернизируются для других конкретных случаев.

Пусть выработана псевдослучайная последовательность битов с периодом $\lambda = 2^t$, где $t$ –число, определяемое количеством битов, в зависимости от длины периода.

Для проверки степени случайности битов в блоке псевдослучайной последовательности, вначале определяются следующее:

1) Возможные элементы, содержащиеся в псевдослучайной последовательности битов, являются “0” и “1” , т.е. ( $s$ ) : 0, 1;

2) Вероятность того, что эти элементы содержатся/появляются в блоке псевдослучайной последовательности равны ( $p_s$ ) : $\frac{1}{2}$, $\frac{1}{2}$;

3) Наблюдаемое число ( $Y_s$ ) : $N_0, N_1$; где $N_0$ и $N_1$ количество нулей «0» и единиц «1» в исходном блоке битов длиной $\lambda = 2^t$ псевдослучайной последовательности $c_1c_2c_3c_4 \ldots c_8c_9 \ldots$, и имеет место равенство $N_0 + N_1 = \lambda$ ;

4) Наблюдаемое число ( $\lambda p_s$ ) : $\frac{\lambda}{2}$., $\frac{\lambda}{2}$;

в табличном виде выражается

| $s$ | 0 | 1 |
|---|---|---|
| $p_s$ | $\frac{1}{2}$ | $\frac{1}{2}$ |
| $Y_s$ | $N_0$ | $N_1$ |
| $\lambda p_s$ | $\frac{\lambda}{2}$ | $\frac{\lambda}{2}$ |

Вычисляется значение «Хи-квадрат» распределения по формуле:

$$V = \sum_{s=0}^{k-1} \frac{(Y_s - np_s)^2}{np_s}.$$

В рассматриваемом случае: $k = 2;\ s \in \{0;1\};\ p_0 = p_1 = \frac{1}{2};\ Y_0 = N_0;\ Y_1 = N_1;\ n = \lambda = 2^t;$

следовательно, по формуле имеется

$$V = \frac{(Y_0 - 2^{t-1})^2 + (Y_1 - 2^{t-1})^2}{2^{t-1}}.$$

По вычисленному значению $V$ определяется степень случайности выработанной последовательности. Для этого воспользуемся таблицей критических точек «Хи-квадрат» критерия распределения случайных величин. По строке $N = k - 1 = 2 - 1 = 1$ этой таблицы находится интервал, где расположено значение $V$ . Если это значение лежит между $p = 25\%$ и $p = 75\%$, то выработанная псевдослучайная последовательность принимается как случайная. Для полноты изложения приводится таблица критических точек «Хи-квадрат» критерия распределения случайных величин

Таблица 2. Таблица критических точек

| | *p*=1% | *p*=5% | *p*=25% | *p*=50% | *p*=75% | *p*=95% | *p*=99% |
|---|---|---|---|---|---|---|---|
| *N=1* | 0.00016 | 0.00393 | 0.1015 | 0.4549 | 1.323 | 3.841 | 6.635 |
| *N=2* | 0.02010 | 0.1026 | 0.5754 | 1.386 | 2.773 | 5.991 | 9.210 |
| *N =3* | 0.1148 | 0.3518 | 1.213 | 2.366 | 4.108 | 7.815 | 11.34 |
| *N =4* | 0.2971 | 0.7107 | 1.923 | 3.357 | 5.385 | 9.488 | 13.28 |
| *N =5* | 0.5543 | 1.1455 | 2.675 | 4.351 | 6.626 | 11.07 | 15.09 |
| *N =6* | 0.8721 | 1.635 | 3.455 | 5.348 | 7.841 | 12.59 | 16.81 |
| *N =7* | 1.239 | 2.167 | 4.255 | 6.346 | 9.037 | 14.07 | 18.48 |
| *N =8* | 1.646 | 2.733 | 5.071 | 7.344 | 10.22 | 15.21 | 20.09 |
| *N =9* | 2.088 | 3.325 | 5.899 | 8.343 | 11.39 | 16.92 | 21.67 |
| *N =10* | 2.558 | 3.940 | 6.737 | 9.342 | 12.55 | 18.31 | 23.21 |
| *N =11* | 3.053 | 4.575 | 7.584 | 10.34 | 13.70 | 19.68 | 24.72 |
| *N =12* | 3.571 | 5.226 | 8.438 | 11.34 | 14.85 | 21.03 | 26.22 |
| *N =15* | 5.229 | 7.261 | 11.04 | 14.34 | 18.25 | 25.00 | 30.58 |
| *N =20* | 8.260 | 10.585 | 15.45 | 19.34 | 23.83 | 31.41 | 37.57 |
| *N =30* | 14.95 | 18.49 | 24.48 | 29.34 | 34.80 | 43.77 | 50.89 |
| *N =50* | 29.71 | 34.76 | 42.94 | 49.33 | 56.33 | 67.50 | 76.15 |
| *N >50* | $v+\sqrt{2v}\,x_p+\frac{2}{3}x_p^2-\frac{2}{3}+O(\frac{1}{\sqrt{v}})$ | | | | | | |
| $x_p$=8 | -2.33 | -1.36 | -0.674 | 0.00 | 0.674 | 1.64 | 2.33 |

Хотя, на основе «Хи-квадрат» критерия получен положительный результат по случайности, не будет лишним проверка и по другим тестам. Чем больше положительных ответов, тем лучше.

Коротко остановимся для проверки степени случайности пары битов в блоке последовательности ключа гаммирования [35-43]. Для этого вначале определяются следующие параметры:

1) Возможные элементы, содержащиеся в псевдослучайной последовательности пары битов, являются «00», «01», «10» и «11», т.е. ( $s$ ) : 00, 01, 10, 11;

2) Вероятность того, что эти элементы содержатся/появляются в блоке псевдослучайной последовательности равны ( $p_s$ ) : $\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}$;

3) Наблюдаемое число ( $Y_s$ ) : $N_{00}, N_{01}, N_{10}, N_{11}$; где $N_{00}, N_{01}, N_{10}$ и $N_{11}$–количества элементов «00», «01», «10» и «11» в исходном блоке битов длиной $\lambda = 2^t$ псевдослучайной последовательности $c_1c_2c_3c_4 \ldots c_8c_9 \ldots$, и имеет место равенство $N_{00}+N_{01}+N_{10}+N_{11}=\frac{\lambda}{2}$ ;

4) Наблюдаемое число ( $\lambda p_s$ ) : $\frac{\lambda}{8}, \frac{\lambda}{8}, \frac{\lambda}{8}, \frac{\lambda}{8}$;

в табличном виде выражается

| $s$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| $p_s$ | $\frac{1}{4}$ | $\frac{1}{4}$ | $\frac{1}{4}$ | $\frac{1}{4}$ |
| $Y_s$ | $N_{00}$ | $N_{01}$ | $N_{10}$ | $N_{11}$ |
| $\frac{\lambda}{2}p_s$ | $\frac{\lambda}{8}$ | $\frac{\lambda}{8}$ | $\frac{\lambda}{8}$ | $\frac{\lambda}{8}$ |

Имея следующие значения параметров:

$k=4;\ s\in\{00;01;10;11\};\quad p_0=p_1=p_2=p_3=\frac{1}{4};\quad Y_0=N_{00};\ Y_1=N_{01};\ Y_2=N_{10};\ Y_3=N_{11};\quad n=\frac{\lambda}{2}=2^{t-1};$

$N=k-1=4-1=3;$ можно осуществить приложение «Хи-квадрат» критерия для определения степень случайности, последовательности пары битов в блоке псевдослучайной последовательности, аналогично как выше.

**Анализ полученных результатов.** Таким образом, необходимые условия по обеспечению стойкости алгоритмов непрерывного шифрования, их обоснованные свойства, математические подходы и модели проверки приведенных необходимых условий стойкости, предложенные криптографические принципы и средства позволяют проводить корректные исследования преобразований алгоритмов.

Определен способ нахождения $\lambda$-длины периода псевдослучайной последовательности.

Разработана модель метода практического приложения «Хи-квадрат» критерия для определения степени случайности элементов или их объединений в блоке выработанной псевдослучайной последовательности.

**Заключение.** Полученные результаты позволяют обеспечить эффективно и научно обоснованно исследовать стойкость алгоритмов непрерывного шифрования. Математические подходы, методы и модели, криптографические принципы и средства, позволяют исследовать криптографические преобразования по соответствующим критериям.

Анализ преобразований алгоритмов класса непрерывного шифрования по критериям сформулированного утверждения системным образом периодически углубляется и расширяется с развитием достижений науки, вычислительной техники и развитием технологий.

## ИСПОЛЬЗОВАННЫЕ ЛИТЕРАТУРЫ

1. Шнайер, Б. (2002). Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си. *М.: Триумф, 816,* 3.
2. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. (2002). Основы криптографии: Учебное пособие, 2-е изд. –М.: Гелиос АРВ, 480 с.
3. Шеннон, К. (1963). *Работы по теории информации и кибернетике*. Рипол Классик.
4. Merkle, R. C. (1978). Secure communications over insecure channels. *Communications of the ACM*, *21*(4), 294-299.
5. Харин, Ю. С., Берник, В. И., Матвеев, Г. В., & Агиевич, С. В. (2003). Математические и компьютерные основы криптологии.
6. Ростовцев, А. Г., & Маховенко, Е. Б. (2005). Теоретическая криптография. *СПб.: АНО НПО «Профессионал*.

7. Молдовян А. А., Молдовян Н. А., Советов Б. Я. (2001). Криптография. – Санкт-Петербург, Изд. «Лань»,. 224 с.
8. Акбаров, Д. Е., & Умаров, Ш. А. (2020). Анализ приложения логических операций к криптографическим преобразованиям средств обеспечения информационной безопасности. *Universum: технические науки*, (2-1 (71)).
9. Akbarov D. E., Umarov Sh. A. (2020). The Application of Logical Operations and Tabular Transformation in the Base Assents of Hash-Function Algorithms. – Computer Reviews Jurnal. Vol. 6 ISSN: 2581-6640. 11-18. Pp.
10. Akbarov, D. E., & Umarov, S. A. (2021). Mathematical characteristics of application of logical operations and table substitution in cryptographic transformations. *Scientific-technical journal*, *4*(2), 6-14.
11. Умаров, Ш. А., & Акбаров, Д. Е. (2016). Разработка нового алгоритма шифрования данных с симметричным ключом. *Журнал Сибирского федерального университета. Техника и технологии*, *9*(2).
12. Акбаров, Д. Е., Умаров, Ш. А., & Акбаров, Д. Є. (2016). Новый алгоритм блочного шифрования данных с симметричным ключом.
13. Akbarov D. E. (2009). Cryptographic methods of ensuring information security and their application. p. 432.
14. Молдовян, Н. А. (2004). *Криптография: от примитивов к синтезу алгоритмов*. БХВ-Петербург.
15. Молдовян, А. А. (2002). *Криптография. Скоростные шифры*. БХВ-Петербург.
16. Hayotov, A., & Rasulov, R. (2021, July). Improvement of the accuracy for the Euler-Maclaurin quadrature formulas. In *AIP Conference Proceedings* (Vol. 2365, No. 1, p. 020035). AIP Publishing LLC.
17. Абдурахманов, К. Х. (2019). Экономика труда теория и практика.
18. Бодров, А. Н. (2009). Прогнозирование рынка труда и стимулы занятости. *Научные исследования в образовании*, (8).
19. Смирнов, В. В. (2011). Оптимизация процесса функционирования рынка труда в условиях неустойчивой экономики. *Вестник Чувашского университета*, (2).
20. Tashpulatov A. (2020). Modeling the supply of labor in the rural labor market. EPRA International Journal of Research and Development (IJRD), 05, pp.150-152, Journal DOI: https://doi.org/10.36713/epra2016 www.eprajournals.com
21. Tashpulatov A. (2020). The use of simulation modeling in forecasting the labor market development International Journal of Research in Economics and Social Sciences(IJRESS) Available online at: http://euroasiapub.org Vol. 10 Issue 8, August- 2020 ISSN(o): 2249-7382 | Impact Factor: 7.077|, P.4-8 http://euroasiapub.org
22. Туктамышева, Л. М. (2018). Математические модели регионального рынка труда: оперативный мониторинг и прогнозирование. *Азимут научных исследований: экономика и управление*, *7*(2 (23)).
23. Хавинсон, М. Ю. (2016). Моделирование динамики численности занятых, безработных и экономически неактивного населения в регионе с учетом социальных связей. *Вестник Воронежского государственного университета. Серия: Экономика и управление*, (4), 178-188.

24. Холмуминов Ш.Р. (2014). Формирование и развитие сельского рынка труда а также их прогнозирование. Монография. Ташкент: “Fan va texnologiya”, 232 p.
25. Abdurazakov, A., Makhmudova, N., & Mirzamakhmudova, N. (2021). On one method for solving degenerating parabolic systems by the direct line method with an appendix in the theory of filration.
26. Абдуразаков, А., Махмудова, Н., & Мирзамахмудова, Н. (2020). Численное решение методом прямых интеграла дифференцирования уравнений, связанных с задачами фильтрации газа. *Universum: технические науки*, (7-1 (76)), 32-35.
27. Абдуразаков, А., Махмудова, Н., & Мирзамахмудова, Н. (2019). Решения многоточечной краевой задачи фильтрации газа в многослойных пластах с учетом релаксации. *Universum: технические науки*, (11-1 (68)).
28. Shadimetov, K., & Daliyev, B. (2021, July). Composite optimal formulas for approximate integration of weight integrals. In *AIP Conference Proceedings* (Vol. 2365, No. 1, p. 020025). AIP Publishing LLC.
29. Шадиметов, Х. М., & Далиев, Б. С. (2020). Коэффициенты оптимальных квадратурных формул для приближенного решения общего интегрального уравнения Абеля. *Проблемы вычислительной и прикладной математики*, (2 (26)), 24-31.
30. Hayotov, A. R., Bozarov, B. I., & Abduganiev, A. (2018). Optimal formula for numerical integration on two dimensional sphere. *Uzbek Mathematical Journal*, *3*, 80-89.
31. Bozarov, B. I. (2019). An optimal quadrature formula with sinx weight function in the Sobolev space. *Uzbekistan academy of sciences vi romanovskiy institute of mathematics*, 47.
32. Hayotov, A., & Bozarov, B. (2021, July). Optimal quadrature formulas with the trigonometric weight in the Sobolev space. In *AIP Conference Proceedings* (Vol. 2365, No. 1, p. 020022). AIP Publishing LLC.
33. Alimjonova, G. (2021). Modern competencies in the techno-culture of future technical specialists. *Current research journal of pedagogics (2767-3278)*, *2*(06), 78-84.
34. Каримов, Ш. Т., & Хожиакбарова, Г. (2017). Аналог задачи гурса для одного неклассического уравнения третьего порядка с сингулярным коэффициентом. *Toshkent shahridagi turin politexnika universiteti*, 121.
35. Fayzullayev, J. I. (2020). Mathematical competence development method for students through solving the vibration problem with a maple system. *Scientific Bulletin of Namangan State University*, *2*(8), 353-358.
36. Mirzakarimov, E. M., & Faizullaev, J. I. (2019). Method of teaching the integration of information and educational technologies in a heterogeneous parabolic equation. *Scientific Bulletin of Namangan State University*, *1*(5), 13-17.
37. Tillabayev, B., & Bahodirov, N. (2021). Solving the boundary problem by the method of green's function for the simple differential equation of the second order linear. *ACADEMICIA: An International Multidisciplinary Research Journal*, *11*(6), 301-304.
38. KOSIMOV, H., & TILLABAEV, B. (2018). Mixed fractional order integral and derivatives for functions of many variables. *Scientific journal of the Fergana State University*, *1*(2), 5-11.
39. Ахмедова, Г. А., & Файзуллаев, Ж. И. (2014). Управление инновационной активностью промышленных предприятий на основе эффективных методов ее оценки и стимулирования. *Актуальные проблемы гуманитарных и естественных наук*, (4-1).
40. Fayzullaev, J. (2020). A systematic approach to the development of mathematical competence among students of technical universities. *European Journal of Research and Reflection in Educational Sciences*

*Vol*, *8*(3).

41. Ernazarov, A. A. (2020). The relevance of the use of computer-aided design systems for teaching students of higher educational institutions. *Scientific Bulletin of Namangan State University*, *2*(8), 348-353.
42. Mirzakarimov, E. M., & Fayzullaev, J. S. (2020). Improving the quality and efficiency of teaching by developing students* mathematical competence using the animation method of adding vectors to the plane using the maple system. *Scientific Bulletin of Namangan State University*, *2*(9), 336-342.
43. Nazarova, G. (2021). Methods of directing economics to scientific research activities. *Current research journal of pedagogics (2767-3278)*, *2*(06), 90-95.