applicability for the solution of predictive problems in the exploration of hydrocarbons is given. The application of these methods allowed reducing the dimension of the original attribute space without losing information. The obtained results of the parameter prediction using these statistical methods are quite stable, which is confirmed by the results of the correlation dependencies and the cross-validation method.

After examining the results, of the statistical analysis of the control data set, it was found that the methods of the principal components and factor analysis were similar in terms of the results obtained. On the one hand, this may indicate that it is sufficient to use one of these methods when processing an input file with geological and geophysical information, but on the other hand, new data sets may have special functional dependencies (new types of traps, reservoir fields, etc.).

Therefore, the hybrid use will give the most insight into the seismic attributes under study in a particular reservoir data set.

In addition, it is considered relevant to investigate the effectiveness of the neural network approach to solve the above mentioned problem.
2002 - Ukrainian national standard. Creating an electronic digital signature based on
elliptic curves includes the generation of key pairs (private and public key), calculation
of signature parameters and its verification.

1. Key generation

Before generating digital signature settings, a private key must be generated. The
public key is derived from the private key and some of the parameters described
below. The key pair must be in the authenticator's memory. As the name implies, a
private key is inaccessible to anyone but its owner, unlike a public key, which must
be public to read. We generate a random number that becomes a private key \( d \) (a
scalar quantity). Next, the public key \( Q(x, y) \) is calculated accordingly:
\[
Q(x, y) = d \ast G(x, y),
\]
where \( G(x, y) \) correspond to the \( x \) and \( y \) coordinates of this base point.

2. Calculation of electronic signature parameters

A digital signature allows the recipient of the message to verify the authenticity
of the message with a public key.
First, our message is converted to a fixed

length message \( h(m) \) using a secure hashing algorithm. To calculate the hash, the developer can use, for example, any of
the SHA algorithms (SHA-1, SHA-2, SHA-3) or any other, providing it meets certain
requirements.

The signature consists of two integers \( r \) and \( s \). The following equation describes
the calculation of \( r \) from the random number \( k \) and the base point \( G(x, y) \):
\[
(x_1, y_1) = k \ast G(x, y) \mod p
\]
\[
r = x_1 \mod n
\]

It should be noted that \( r \) must not be zero. Otherwise, when \( r \) is 0, a new random
number must be generated, and \( k \) and \( r \) must be calculated again.
After calculating \( r \), we calculate \( s \) according to the following equation, using scalar
operations. Inputs are the message \( h(m) \); private key \( d \); \( r \); and a random number \( k \):
\[
s = (k^{-1}(h(m) + d \ast r)) \mod n
\]
For a signature to be "valid", \( s \) cannot be zero. If \( s \) is 0, a new random number
\( k \) must be generated, and both \( r \) and \( s \) must be calculated again.

3. Signature verification

The signature verification is analogous to the previous paragraph. Its purpose
is to verify the authenticity of the message using the public key of the authenticator.
Using the same secure hash algorithm as in the signing step, \( h(m) \) is calculated and
signed by the authenticator together with the public key \( Q(x, y) \).
The input data is the message \( h(m) \), the public key \( Q(x, y) \), the signature
components \( r \) and \( s \) and point \( G(x, y) \):
\[
w = (s - 1) \mod n
\]
\[
u_1 = (h(m) \ast w) \mod n
\]
\[
u_2 = (r \ast w) \mod n
\]
\[
(x_2, y_2) = (u_1 \ast G(x, y) + u_2 \ast Q(x, y)) \mod n
\]
The check is successful if \( x_2 \) is equal to \( r \), thus confirming that the signature
was indeed computed using a private key.

According to the standard DSTU 4145-2002 the algorithm of elliptic curves
is centered on fields of the characteristic described by the equation \( y^2 + xy = x^3 + ax^2 + b \), \( b \neq 0 \). Another difference is that arithmetic operations are performed on
polynomials, not on numbers. According to the standard, mathematical operations
can be implemented on a polynomial basis or on an optimal normal basis. Consider
the first option:
We set the following parameters for the algorithm: $A, B$ are the coefficients of the equation of the elliptic curve, which was given above. $k, m$ - the degree of the main polynomial, the modulus of which performs all arithmetic operations. For example, when $k = 5, m = 5$, we obtain a polynomial of the form: $x^5 + x^3 + x^2 + x + 1$.

$P$ - Basepoint of order $n$.

The key pair consists of the secret key $d$ and the public key $Q = -d \cdot P$.

**Formation of electronic digital signature:**

1. We generate a certain number $a$, such that $1 < a < n$.
2. Calculate the point $R = a \cdot P$.
3. Calculate the polynomial $f_r = R_x \cdot h(M)$, where $R_x$ is the $x$-coordinate of the point $R$; $h(M)$ - hash from the message $M$.

We represent $f_r$ as the number $r$.

Calculate the number $s = (a + d \cdot r) \pmod n$.

As a result, the pair $(r, s)$ is our signature.

To verify the signature, the following is performed:

1. We represent the signature as a pair of numbers $(r, s)$;
2. Calculate the point of the curve $R = s \cdot P + r \cdot Q$;
3. Calculate the element of the main field $f_r = h(M) \cdot R_x$;
4. Represent $f_r$ as the number $r_1$.

If the equality $r_1 = r$, is satisfied, then the signature is valid.

In conclusion, we would like to emphasize that, despite certain shortcomings of elliptic curves, such as the "weakness" of a large group of elliptic curves and the complexity of the algorithm in mathematical terms, they have undeniable advantages. We need a much shorter key length compared to the "classical" asymmetric cryptography, which increases the efficiency of calculations. In addition, the speed of elliptic algorithms is much higher than that of classical ones. Due to the small key length and high speed of operation, asymmetric cryptography algorithms on elliptic curves can be used in smart cards and other devices with limited computing resources. The advantages of elliptic cryptography are derived from one specific fact: for the discrete logarithm problem on elliptic curves, there are no sub-exponential decision algorithms, which allows the reduction of the key length and an increased productivity.

**References:**

[1] (2012) Secure Hash Standard (SHS). National Institute of Standards and Technology [Online]. Available at: https://csrc.nist.gov/csrc/media/publications/fips/180-4/final/documents/fips180-4-draft-aug2014.pdf

[2] ELLIPTIC CURVE DIGITAL SIGNATURE ALGORITHM EXPLAINED [Online]. Available at: https://www.maximintegrated.com/en/design/technical-documents/tutorials/5/5767.html

[3] An Elliptic Curve Cryptography based Authentication and Key Agreement Protocol for Wireless Communication', in (ed.). Corvallis, USA: Oregon State University

[4] ЭЦП стран СНГ на Python. Available at: https://habr.com/ru/company/virgilsecurity/blog/301048

[5] Цифровий підпис, що ґрунтується на еліптичних кривих. Формування та перевірка. ДСТУ 4145 - 2002., Kyiv,Ukraine.