The actual task of forming the quantitative assessment of the degree of protection of ACSs information resources, which would be the reference value in estimation of the effectiveness of protective measures taken.

The following method is proposed:

1. Preliminary analysis of the ACS and information resources (data) circulating in it, in order to obtain baseline data for assessment:
   • the list of nodes and units \( Z_i \) allocated in the ACS, \( i=1\ldots s \), \( s \) is the total number of ACS nodes;
   • the list of data resources processed by the ACS (general and per-node).
2. Ranking of nodes and units of ACS by groups according to the value of the data processed by them.
3. Formation of the numerical assessment of the protection degree for information resources of the ACS, taking into account their value and the degree of criticality of the data integrity, accessibility and confidentiality.
1) **At first** it is necessary to decompose the researching ACS into key nodes. It is necessary to separate nodes of:
- lower (field) level (sensors, actuators, etc.),
- medium level (programmable logic controllers),
- top level (operator's terminal, servers, etc.).

2) **At the next stage**, there is the local task of distributing the identified information resources of the ACS, as well as the nodes involved in their processing, according to the degree of security importance depending on their value.

Based on the list of ACS information resources and the given rating scale, experts should estimate the cost of the \( j \)-th information resource circulating in the system. In case of difficulties in obtaining a specific numerical assessment from an expert, it is possible to offer a certain value range and go to relative indicators:

\[
C_j = \frac{C_{j_{\text{min}}} \gamma_1 + C_{j_{\text{max}}} \gamma_2}{(\gamma_1 + \gamma_2)(C_{j_{\text{min}}} + C_{j_{\text{max}}})}
\]

where \( \gamma_1 \) and \( \gamma_2 \) are empirical coefficients;
\( j = 1 \ldots m \), \( m \) is the total number of information resources allocated to the ACS.
Then the indicator of the value of the \( j \)-th ACS information resource:

\[
q_j^C = C_j / (\max_j C_j)
\]

The indicator of the value of information resources for the specific \( i \)-th node ACS \( Z_i \) is defined as:

\[
Q_i^C = \max_{j \in Z_i} q_j^C
\]

where \( q_j^C \) - the value of the \( j \)-th ACS information resource.

As a result, the generalized matrix of indicators of the data value for all selected nodes \( i \) of the considered ACS is obtained:

\[
Q^C = \begin{pmatrix}
Z_1^C & Z_i^C & Z_s^C \\
Q_1^C & Q_i^C & Q_s^C
\end{pmatrix}
\]

The resulting matrix (4) allows to rank the nodes and units of the ACS according to the value of the data they process by groups: especially important, important, medium and low importance.
3) **At the third stage**, the desired indicator of the required degree of ACS data security is obtained. The indicator should take into account quantitative estimates of the degree of criticality of violations of confidentiality, integrity, and accessibility for each selected node and unit of the ACS.

As a result of the processing of expert information, we obtain the summary matrix of criticality estimates of such type:

\[
\begin{bmatrix}
Q_{\text{conf}}^X & Q_{\text{acc}}^X & Q_{\text{in}}^X \\
Z_1 & q_{\text{conf}}^1 & q_{\text{acc}}^1 & q_{\text{in}}^1 \\
Z_2 & q_{\text{conf}}^2 & q_{\text{acc}}^2 & q_{\text{in}}^2 \\
\end{bmatrix}
\]

where \( Z_i \) is the \( i \)-th node of the ACS, \( q_{\text{conf}}^i = [0-1], \ q_{\text{acc}}^i = [0-1], \ q_{\text{in}}^i = [0-1] \) are the degree coefficients of violation of information security properties.

For groups of important \( Z_{im} \) and especially important \( Z_{elim} \) nodes during the formation of indicators \( P_{\text{elim}}^{Z_{im}} \) and \( P_{\text{elim}}^{Z_{elim}} \), the multiplicative convolution of found indicators \( Q_{\text{conf}}^X, Q_{\text{acc}}^X, Q_{\text{in}}^X \), should be used, since the contribution of each of them to the overall assessment is extremely critical:

\[
P_{\text{elim}}^{Z_{im}} = \left( \prod_{i=1}^{s_{im}} \left( \frac{q_{\text{conf}}^i + q_{\text{acc}}^i + q_{\text{in}}^i}{3} \right) \right)^{1/k}, \quad P_{\text{elim}}^{Z_{elim}} = \left( \prod_{i=1}^{s_{elim}} \left( \frac{q_{\text{conf}}^i + q_{\text{acc}}^i + q_{\text{in}}^i}{3} \right) \right)^{1/k}
\]

where \( s_{im}, s_{elim} \) - the number of ACS nodes in the groups of important and especially important, respectively; \( k \) - is coefficient taking into account the degree of sensitivity of the overall assessment to the indicators of this group.

For estimating the indicators \( P_{\text{elim}}^{Z_{im}} \) and \( P_{\text{elim}}^{Z_{elim}} \) for the ACS nodes, assigned to the groups of the medium \( Z_{min} \) and low importance \( Z_{lim} \), the additive convolution of the estimates is used:

\[
P_{\text{elim}}^{Z_{im}} = \left( \sum_{i=1}^{s_{im}} \left( \frac{q_{\text{conf}}^i + q_{\text{acc}}^i + q_{\text{in}}^i}{3} \right) \right)^{1/2}
\]

\[
P_{\text{elim}}^{Z_{lim}} = \frac{\sum_{i=1}^{s_{lim}} (q_{\text{conf}}^i + q_{\text{acc}}^i + q_{\text{in}}^i)}{s_{lim}}
\]

Then the generalized indicator \( P_{\text{ACS}}^{\text{acs}} \) of the protection degree for ACS information resources, taking into account the weights \( W_{elim}, \ W_{im}, \ W_{min}, \ W_{lim} \) of each group of indicators, is defined as:

\[
P_{\text{acs}}^{\text{acs}} = W_{elim} P_{\text{elim}}^{Z_{im}} + W_{im} P_{\text{elim}}^{Z_{elim}} + W_{min} P_{\text{elim}}^{Z_{min}} + W_{lim} P_{\text{elim}}^{Z_{lim}}
\]

where \( \sum W_i = 1 \).
The paper deals with the features of ACSs as objects of data protection, suggests the approach to isolating its components as part of analyzing and assessing the protection grade that must be ensured for high-quality and efficient system operation.

The result of applying the described method is obtaining of quantitative indicators of the protection degree for especially important $P^{z_{im}}$, important $P^{z_{im}}$, medium $P^{z_{min}}$ and low important $P^{z_{lim}}$ ACSs nodes, taking into account the value and criticality of the integrity, accessibility and confidentiality of the data they process. On the basis of these indicators, a generalized indicator $P^{ACS}$ of the required degree of ACS information resources protection was obtained.