# Şapte nivele de protecţie a datelor în sistema de evidenţă a resurselor energetice BALANCE

**Protecţia IoT** de multe ori este înerpretată ca focalul de eşecuri. Cu toate acestea, se înregistrează progrese serioase în acest domeniu și multe companii se străduiesc să rezolve problemele comune care duc la eșecuri în materie de securitate, adesea în știri. Iată câteva exemple de probleme întâlnite în domeniul securității Internetului și metodele dezvoltate de DJV-COM pentru a le rezolva.

**Şapte niveluri de protecție a datelor:**

**La nivelul de acces la Internet - baza de date.** Для администратора, операторов и пользователей – пароль с распределением прав на уровне объектов. Реализация «облачный сервис» с отсутствием прямого доступа к данным. Весь сервис реализуется на базе API интерфейса.
**La nivelul de acces a concentratorului - baza de date.** Pentru administratori, operatori și utilizatori, o parolă cu distribuirea drepturilor la nivelul obiectului. Implementarea "serviciului de tip cloud" cu lipsa accesului direct la date. Întregul serviciu este implementat pe baza interfeței API.
**La nivelul modulului radio - concentrator.** Rețelele sunt împărțite în adrese logice, neștiind care este imposibilitatea realizării schimbului de date în rețeaua radio. În plus, este utilizată o semnătură digitală. Clientul are posibilitatea de a schimba adresa rețelei logice.
**La nivelul modulului radio - dispozitivul de evidenţă.** Folosirea unei ieșiri de puls pentru a scoate informații din dispozitivul de evidenţă **nu va fi posibil de "spart" fundamental contorul** – pentru a modifica datele sau pentru a întrerupe funcționarea contorului. În plus, conexiunea este monitorizată pentru integritate - înrerupere ţi scurt circuit..
**La nivelul modulului radio** – nu există nicio comandă pentru modificarea datelor acumulate pe modulul radio. Acumularea datelor se face prin analogie cu un dispozitiv mecanic de citire - numai în direcția acumulării. **Nu există instrucțiuni pentru resetarea contorului sau schimbarea acestuia.**
**La nivelul bazei de date.** Dublarea, copierea de rezervă și validarea datelor.
**La nivel de Analiză.** Monitorizarea debitului maxim pentru o oră și o zi, controlul uniformității creșterii datelor, controlul lipsei de date. În plus, controlul unical a adreselor de rețea ale modulelor radio și duplicarea pachetelor de date.

**Analizăm posibilitatea înlocuirii dispozitivelor.** Principalul atac este următorul: inamicul creează un dispozitiv care simulează hardware-ul din rețeaua IoT și folosește dispozitivul nou creat pentru a livra date false către rețeaua IoT.
**Dacă nu există un astfel de dispozitiv în rețea**, acesta nimerește în secțiunea UNKNOWN și operatorul sau administratorul de rețea trebuie să determine unde aparține aparatul respectiv.
**Dacă acest dispozitiv nu este cunoscut operatorului,** acesta va rămâne în secțiunea UNKNOWN.
**Dacă acest dispozitiv este cunoscut rețelei** – se monitorizează unicitatea adreselor de rețea ale modulelor radio și duplicarea pachetelor de date, prin urmare sistemul va da o eroare - duplicarea dispozitivelor. În plus, fiecare dispozitiv are legătură cu concentratorul său, adică Nu puteți trimite un pachet de la un alt concentrator - sistemul va avertiza administratorul.

# Seven levels of data protection in the AMR/AMI system BALANCE

**IoT security** is often perceived as a hotbed of failures. Nevertheless, great progress is being made in this area, and many companies are working to solve common problems that lead to security failures, which are often in the news. Here are just a few examples of problems encountered in the field of IoT security, and methods developed by DJV-COM to solve them.

**Seven levels of data protection:**

**At the level of access via the Internet - the database**. For administrators, operators and users, a password with rights distribution at the object level. Implementation of the "cloud service" with the lack of direct access to data. The whole service is implemented on the basis of the API interface.
**At the access level, the concentrator - the database.** Two levels of protection - the first concentrator goes to a pre-defined IP, regardless of where the connection is initiated. The second level of protection is a private SSL connection protocol on the IP connection.
**At the level of the radio module - the concentrator.** Networks are divided into logical addresses, not knowing which it is impossible to realize the data exchange in the radio network. Additionally, a digital signature is used. The customer has the opportunity to change the logical address of the network.
**At the level of the radio module - the metering device.** Using a pulse output to remove information from the meter **does not allow you to fundamentally "hack" the meter** - to change the readings or disrupt the functioning of the meter. Additionally, the connection is monitored for integrity - open and short.

**At the radio module level** - there is basically no command for changing the accumulated data on the radio module. Accumulation of data is carried out by analogy with a mechanical reading device - only towards accumulation. There are no instructions for resetting the counter or changing it.
**At the database level.** Duplication, backup and data validation.

**At the level of Analytics.** Monitoring of the maximum flow rate for an hour and a day, control of the uniformity of data growth, control of the lack of data. In addition, control of the uniqueness of network addresses of radio modules and duplication of data packets.

**Consider the option of spoofing devices.** The main attack is as follows: the enemy creates a device that simulates the hardware in the IoT network and uses its newly created device to feed false data into the IoT network.
**If there is no such device on the network**, it falls into the UNKNOWN section and the operator or network administrator must determine where this device belongs.
**If this device is unknown to the operator**, it will remain in the UNKNOWN section.
**If this device is known to the network**, it controls the uniqueness of network addresses of radio modules and duplicates of data packets, hence the system will give an error - duplication of devices. Additionally, each device has a binding to its concentrator, i.e. you can not send a packet from another concentrator - the system will alert the administrator.