

## ACTUALITATEA SECURITĂȚII BANCARE

**BUNACALEA VASILE, masterand, MI-181m**

Academia de Studii Economice a Moldovei,

Republica Moldova, Chișinău, str. Mitropolit Gavriil Bănulescu-Bodoni 61,

e-mail: vasile.bunacalea@jivygroup.com

**Abstract.** *We live in a modern environment where the financial sector and personal money are important for a good life. So we are in a modern environment where criminals use modern methods for identity theft. Bank fraud is always relevant and has some important impacts at the national level, at the international level. Thus the security of personal data at bank level should be 100% ensured. This study will explain more information on the timeliness of bank fraud, how it is organized the protection of information in banks, and how it could avoid fraud in banks, also will explaining the methods applied by banks to ensure the highest level of data protection.*

**Key words:** *GDPR, data protection, banking operations, bank security, bank fraud.*

**JEL CLASSIFICATION: P000, P430, P490, O350, O310**

### INTRODUCERE

După cum cunoaștem, sectorul financiar, inclusiv infrastructura bancară mereu este cointereseată de către infractori cu scopul de a manipula datele cu caracter personal.

Securitatea este definită drept protecția împotriva amenințărilor de securitate și este denumită „circumstanță, condiție sau eveniment cu potențialul de a provoca dificultăți economice pentru datele sau resursele de rețea sub formă de distrugere, dezvăluire, modificare a datelor, refuz de serviciu. În prezent, în legătură cu evoluția tehnologică aspectul securității bancare a manifestat o evoluție continuă. În dependență de nivelul securității banca păstrează următoarele caracteristici reputația și competitivitatea.[3]

Deci, nivelul înalt de securitate permite minimizarea următoarelor riscuri:

- riscul scurgerii de informații secret oficiale / comerciale / bancare.
- riscul de distrugere și pierderea de date valoroase.
- riscul utilizării în activitățile băncii, inclusiv la acceptare decizii de management, a informații incomplete sau denaturate.
- riscul răspîndirii informațiilor eronate privind activitatea băncii în mediul exterior care influențează negativ asupra reputației bancare.

### CONȚINUTUL DE BAZĂ.

Analizînd un caz particular BC „Moldova Agroindbank” activează din 8 mai 1991. În activitatea sa BC „Moldova Agroindbank”, S.A. asigură respectarea strictă și aplicarea întocmai a legilor și hotărîrilor ce acționează pe teritoriul Republicii Moldova, Legea „Cu privire la instituțiile financiare”, a statutului BC „Moldova Agroindbank” S.A. Deci, analizînd timpul activității sale, banca și-a reafirmat reputația ca fiind una dintre cele mai sigure și mai stabile instituții financiare din țară.

Munca departamentelor bancare este asociată cu acumularea unui număr mare de informații privind datele cu caracter personal a clienților. În mod tradițional, informațiile sunt stocate pe hârtie. Atît timp cît informațiile sunt procesate în modul manual, în acest caz aspectul securității datelor scade dramatic. Procesarea manuală a documentelor bancare prezintă o vulnerabilitate a securității, deoarece documentele care conțin informații cu caracter personal trec prin operatorii bancari și nu prin un sistem informatic securizat și cu un nivel de acces per operator.

În același timp, este dificil de căutat rapid date despre clienți, de asemenea, este dificil de generat rapoarte care includ tranzacțiile clienților. Deci din această problemă reiese crearea unei soluție convenabile pentru automatizarea procesului și aplicarea unei structuri securizate. Aplicația va fi destinată spre utilizare de către managerii, angajații băncii. În scopul eficienței și gestionării

informațiilor privind datele personale ale clienților, este oferită o aplicație cu denumirea «BankingOperations».

«BankingOperations» include următoarele avantaje:

- Formarea rapidă a documentelor operaționale (completarea și tipărirea);
- Căutare rapidă a informații despre clienți și documente;
- Menținerea unei arhive sigure a documentelor;
- Generarea rapoartelor privind operațiunile bancare;
- Integrarea unui nivel dedicat de securitate care include forma de logare și nivel de acces per angajat;

Această aplicație aplică soluția de securizare și protejare a datelor cu caracter personal, sunt combinate soluții tehnice moderne pentru a asigura un nivel de securitate mai ridicat.

Caracteristicile sistemelor informatice bancare sunt că acestea stochează și prelucrează o cantitate mare de date privind starea financiară-contabilă și activitățile operaționale ale persoanelor fizice și juridice.[1] Această caracteristică necesită implicarea nivelului de securitate pentru a asigura protejarea datelor, deci operatorii băncii anunță clienții băncii că datele lor personale sunt protejate după următoarele principii:

- Software antivirus – instalare programelor de protecție;
- Control de acces a sistemului - asigură că persoanele neautorizate nu dețin acces la sistem și nu pot acces datele;
- Limitarea grupului de persoane care au dreptul la procesarea și editarea datelor cu caracter personal a clienților;
- Criptare – informații;

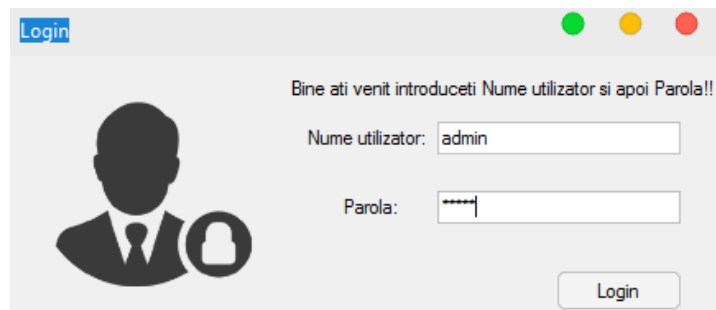
Toate aceste metode sunt conforme cu Regulamentul general european privind protecția datelor.

«GDPR»[2] **În fond, acest principiu al responsabilității și protecției datelor este unul dintre vectorii cheie ai GDPR care este aplicat în bancă. Operatorii de date personale sunt obligați nu numai să respecte aceste principii, ci și să demonstreze modul în care sunt procesate datele privind validarea că principiile de prelucrări a datelor personale sunt respectate.**

Aplicația este foarte intuitivă și simplă pentru angajații băncii și este format din următoarea structură:

- Fereastra de autorizare
- Meniul principal;
- Secțiunea de raportare;
- Secțiunea pentru introducerea datelor și vizualizarea clientului;

Această aplicație are ca scop sporirea protecției datelor cu caracter personal, pentru a respecta acest principiu aplicația include fereastra de autorizare care oferă accesul doar persoanelor care au credențiale corecte, la fel fiecare utilizator are drepturi de acces individual sau pe grupul de persoane. Când datele sunt introduse incorect, este afișat următorul text: "Nume nevalid utilizator sau parolă. "



**Figura 1. Fereastra „Autorizare”**

Pentru a crea o interfață mai simplă, secțiunea meniu principal a fost divizată în următoarea structură:

- prima secțiune este „Clienți”;
- a doua secțiune este „Credite”;

- a treia secțiune este „Administratori”;
- a patra secțiune este „Rapoarte”;
- a cincea secțiune este „Opțiuni”.

Clienți Credite Administrator Rapoarte Opțiuni

**Figura 2 Fereastra de meniu**

Fereastra „Clienți” conține câmpuri pentru toate datele necesare băncii, și a valida înregistrarea unui client nou.

Date Client		Date Credit	
Nume	Gonta Ion	Tip credit	credit imobiliar Prima( v)
Adresa	Chisinau, Maria Dragan 10/1	Perioada	12
IDNO Client	197364840	Suma	500000
Nume Director	Tulbure		
Prenume Director	Ion		
IDNP Director	2546003689710		
Nume Contabil	Cibotaru		
Prenume Contabil	Vasile		
IDNP Contabil	2000036500246		
Telefon	069574354		
Client Salariu (Lunar)	5000		

Introducere

**Figura 3. Fereastra Clienților**

Fereastra „Administratori” această fereastră va permite să adăugați utilizatori noi pentru autentificare, fiecare utilizator trebuie să specifice un nume și o funcție în bancă.

Login	Vasile97
Parola	summer
Nume	Bunacalea
Prenume	Vasile
Functie	Sef_departamen v
Rol	admin v

Introducere

**Figura 4. Fereastra Administratorilor**

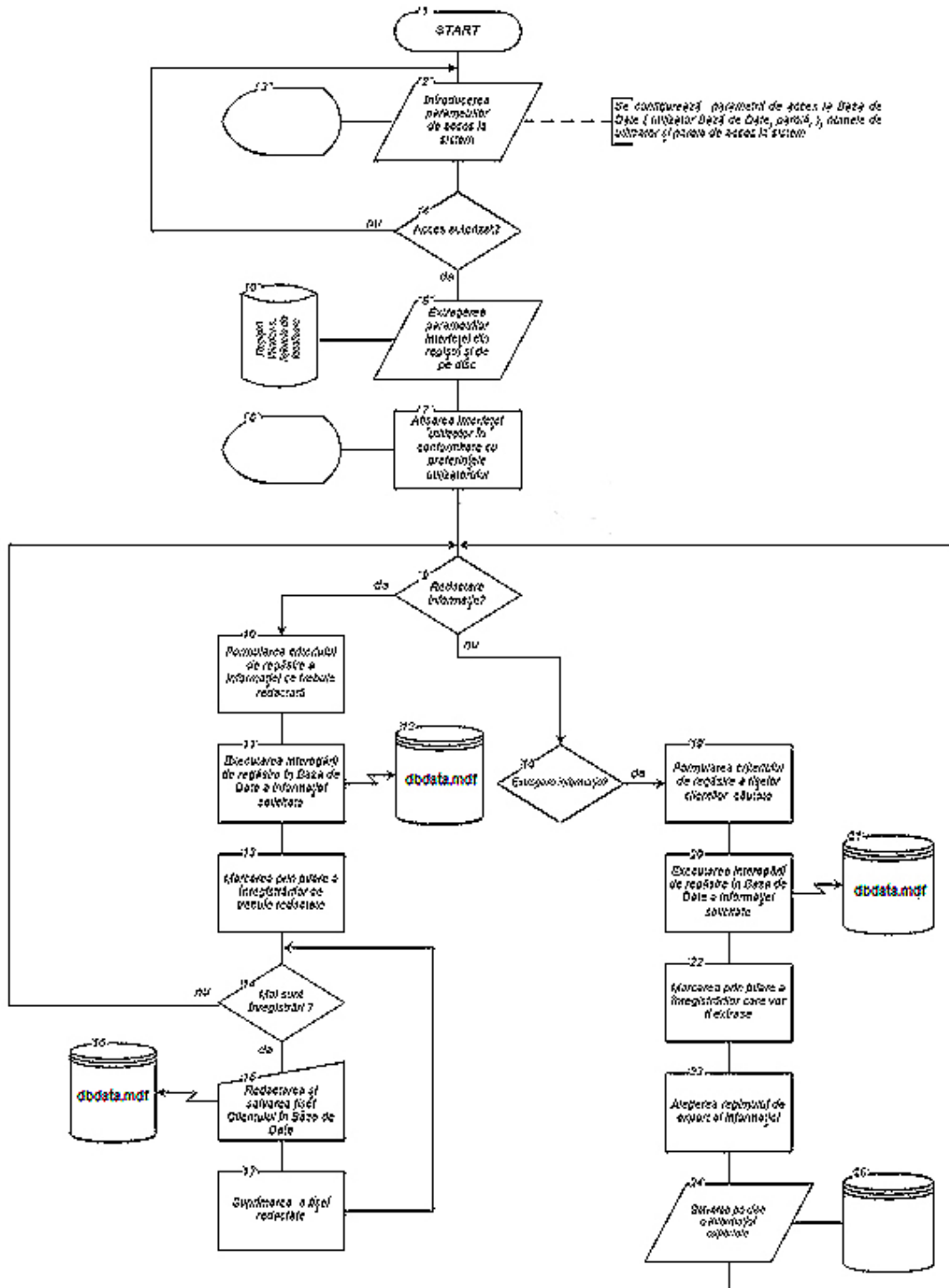


Figura 5. Schema procesului tehnologic de prelucrare a datelor

### CONCLUZII/RECOMANDĂRI.

În baza cercetării au fost definite obiectivele sistemului informatic elaborat, care includ eficientizarea prelucrării informației dar și îmbunătățirea nivelului de securitate privind evidența beneficiarilor de credite bancare. Sistemul informatic trebuie să asigure furnizarea eficientă a informațiilor necesare

conducerii, ceea ce presupune obținerea operativă a informației prelucrate de SI proiectat necesare conducerii.

Rezumînd putem deduce, că într-un mediu modern prelucrarea manuală a datelor trebuie automatizată, sistemul informatic elaborat ne oferă accesul rapid și filtrarea informațiilor din sistem, dar să nu uităm că aplicația oferă un nivel mai sporit de securitate la diferite niveluri de acces.

**REFERINȚE BIBLIOGRAFICE:**

1. A.M. Сычев, П.В. Ревенков, А.Б. Дудка, *Безопасность электронного банкинга*, 2017, 156 p.
2. Dispoziții generale privind protecția datelor cu caracter personal (<https://gdpr-info.eu/>), (accesat la 14.04.2020).
3. Shadi A. Aljawarneh, *Măsuri de securitate bancară online și protecția datelor*, Jordan University of Science and Technology, 2017, 312 p.
4. Rob M., *C# Programming Yellow Book*, UK, 2016
5. *BExpert Documentation Index*, ([www.ibexpert.net/ibe/index.php?n=Doc.Doc](http://www.ibexpert.net/ibe/index.php?n=Doc.Doc)), (accesat la 14.04.2020)

---

**Coordonator științific: OHRIMENCO SERGHEI, dr. hab., prof. univ.,  
Academia de Studii Economice a Moldovei,  
Republica Moldova, Chișinău, str. Mitropolit Gavriil Bănulescu-Bodoni 61,  
e-mail: [osa@ase.md](mailto:osa@ase.md)**