

8. Титков А.Н., Илуридзе А.Н., Миронов И., Чебан В.Н. ФТП, 20 (1), 25, 1986.
9. Бир Г.Л., Аронов А.Г., Пикус Г.Е. ЖЭТФ, 69, 1382, 1975.
10. Bir G. L., Aronov A. G., Pikus G. E. Sov. Phys. JETP, 42, 705, 1976.
11. Глазов М.М., Ивченко Е.Л. ЖЭТФ, 126, 6 (12), 1465, 2004.
12. Madelung O. Semiconductors - basic data. Springer, Berlin, 1996. pp.114-121.  
<http://dx.doi.org/10.1007/978-3-642-97675-9>.
13. Dyakonov M. I, Perel V. I. Theory of optical spin orientation of electrons and nuclei in semiconductors. In: Meier F., Zakharchenya B.P. (Eds.). Optical orientation V.8 Elsevier, Amsterdam, 1984. pp.11-71.  
<http://dx.doi.org/10.1016/B978-0-444-86741-4.50007-X>
14. Plaza J.L., Dieguez E. Cryst. Res. Technol.39, 5, 396, 2003.
15. Georgitse E. I., Gutsulyak L. M., Ivanov-Omskii V. I., Masterov V. F., Smirnov V. A., Yuldashev Sh. U. Sov. Phys. Semicond. 25, 1180, 1991.
16. Georgitse E.I., Gutsulyak L.M., Ivanov-Omskii V.I., Pogorletschy V.M., Titkov A.N. Journal of Technical Physics Letters, 17, 17, 21, 1991 (in Russian).

## **ANALIZA VULNERABILITĂȚII DE SECURITATE A REȚELELOR INFORMAȚIONALE**

**Claudia Hlopanicov**, asistent universitar

Academia Militară a Forțelor Armate “Alexandru cel Bun”

**Abstract.** Vulnerabilitatea este o slăbiciune a sistemului care permite o acțiune neautorizată. Acestea sunt erori care apar în diferite faze ale dezvoltării, respective folosirii sistemelor informaționale.

**Key words.** vulnerabilitate, sistemul informational, rețea de calculatoare.

### **Introducere**

Problemele de securitate din orice tip de rețea de calculatoare provine dintr-o contradicție fundamentală a Internetului și anume caracterul public dorit de utilizatori pentru orice resursă informațională și nevoia de securizare a informațiilor și a rețelei în sine față de atacurile persoanelor rău-intenționate care urmăresc compromiterea, preluarea, modificarea sau distrugerea informațiilor ori întreruperea funcționării rețelei.

Datorită dezvoltării tehnologiei, sistemul informatic a devenit un instrument de comunicare indispensabil. Dar orice mijloc de comunicare, mai ales când mediul de comunicare este un mediu nesigur, cum este Internetul, prezintă riscuri. Utilizarea sistemelor informatice conectate la Internet în domenii diferite precum domeniul militar sau domeniul comercial face ca acest risc să crească.

Sistemele informaționale s-au demonstrat vulnerabile în fața atacurilor de pe Internet, la accesările neautorizate a sistemului, la modificări sau distrugeri de informații, accidentale sau intenționate. Atenuarea și corectarea acestor vulnerabilități a devenit o obligație atât pentru instituții cât și pentru persoanele fizice pentru protejarea informațiilor.

## **Securitatea informațională a rețelelor de calculatoare**

Securitatea se poate pune în aplicare prin diverse metode pornind de la încuierea încăperilor cu calculatoare și a calculatorului însuși, protejarea informației a intrărilor în rețeaua de calculatoare cu parole, folosirea sistemelor de protejare a fișierelor de date pentru împiedicarea distrugerii acestora, criptarea liniilor de comunicații din rețelele de calculatoare și ajunge până la folosirea unor tehnologii speciale pentru împiedicarea interceptării diferitelor radiații emise de echipamentele de calcul în timpul funcționării normale a acestora.

De aceea, informațiile stocate și/sau transmise în/din sistemele de calcul și rețele devin vulnerabile. Internetul este o structură deschisă la care se poate conecta un număr mare de calculatoare, fiind deci greu de controlat. De aceea, putem vorbi de vulnerabilitatea rețelelor, manifestată pe variate planuri. Un aspect crucial al rețelelor de calculatoare, în special al comunicațiilor prin Internet, îl constituie securitatea informațiilor.

În cazul Internet-ului, adresele diferitelor noduri și servicii pot fi determinate ușor. Orice posesor al unui calculator personal cu conectivitate la Internet, având cunoștințe medii de operare poate încerca să forțeze anumite servicii cum ar fi conectarea la distanță cu ajutorul protocoalelor ca telnet, ssh, remote connection, transferul de fișiere FTP (*File Transfer Protocol*, <https://ru.wikipedia.org/wiki/FTP>) sau poștă electronică (e-mail). O rețea de calculatoare este o structură deschisă la care se pot conecta noi tipuri de echipamente. Acest lucru conduce la o lărgire necontrolată a cercului utilizatorilor cu acces nemijlocit la resursele rețelei.

### **Vulnerabilitatea sistemelor informaționale**

Principalele vulnerabilități în cadrul sistemelor informatice sunt de natură fizică, hardware, software sau umană. Din punct de vedere software, există mai multe tipuri de vulnerabilități: care măresc privilegiile utilizatorilor locali fără autorizare, care permit utilizatorilor externi să acceseze sistemul în mod neautorizat și care permit implicarea sistemului într-un atac asupra unui grup de utilizator.

Vulnerabilitatea rețelelor se manifestă pe două planuri:

- *posibilitatea modificării sau distrugerii informației, adică atacul la integritatea ei fizică;*
- *posibilitatea folosirii neautorizate a informațiilor, adică scurgerea lor din cercul de utilizatori stabilit.*

Rețelele sunt ansabluri complexe de calculatoare. Este foarte dificil să se obțină o schemă completă a tuturor entităților și operațiilor existente la un moment dat, astfel încât rețelele sunt vulnerabile la diferite tipuri de atacuri sau abuzuri.

În viitor, rețelele de calculatoare vor deveni o parte esențială din viața socială și individuală. De funcționarea lor corectă depinde activitatea diferitor instituții și chiar personală. Pe măsură ce calculatoarele personale pot fi conectate de acasă în rețele, o serie de activități pot fi făcute de persoane particulare. Luând în considerație, tipurile de date pe care persoanele le pot citi, care sunt celelalte persoane cu care pot comunica și la ce programe au

acces. Tot mai multe informații memorate în fișiere devin posibil de corelat prin intermediul rețelelor.

### **Metode de protecție a sistemelor informatice**

În prezent informația înseamnă puterea, drept pentru care tot mai multe persoane încearcă să obțină informații pe toate căile posibile. Important să cunoaștem cum să protejăm informațiile. Cea mai bună apărare față de acești atacatori este evitarea conexiunii în rețea a sistemelor care conțin informații importante și controlul strict al accesului fizic la acestea.

Conceptele de bază în securizarea unui sistem informatic, sunt următoarele:

- *controlul accesului la sistem* asigură că utilizatorii neautorizați nu pot pătrunde în sistem și încurajează (uneori chiar forțează) utilizatorii autorizați să fie conștienți de necesitatea securizării computerelor. Controlul accesului se extinde de la măsurile primare, la măsuri de jurnalizare (prin menținerea unui log) a tuturor conexiunilor și a operațiilor efectiv executate pe durata conectării. Controlul accesului la date asigură monitorizarea persoanelor care au acces la date, tipul datelor accesate și scopul accesului. Sistemul trebuie să suporte un control selectiv al accesului, permițând unui utilizator să determine dacă alții pot citi sau modifica datele sale. Administrarea sistemului și implementarea politicii de securitate constau în realizarea, planificarea și efectuarea unor proceduri independente care fac un sistem sigur și urmăresc delimitarea cu precizie a responsabilităților administratorului de sistem, instruirea adecvată a utilizatorilor și controlarea lor, pentru a fi siguri că politicile de securitate se respectă. Această categorie implică un management de securitate a computerelor global, prin indicarea amenințărilor cărora trebuie să le facă față sistemul și printr-o evaluare a costurilor de protecție împotriva lor. Arhitectura sistemelor de calcul și a rețelelor de calculatoare, ca rezultat al proiectării sistemului (mai ales într-un sistem informatic care manipulează date confidențiale) are la bază, pe lângă criteriile de performanță și eventual de cost, criterii și reguli clare referitoare la securitatea respectivului sistem.

- *criptarea* este o altă metodă importantă de protejare a informațiilor sensibile stocate în sistemele de calcul, dar și a celor care sunt transmise pe liniile de comunicație. Informațiile care sunt criptate rămân sigure chiar dacă sunt transmise printr-o rețea care nu oferă o securitate intrinsecă puternică deoarece chiar și în cazul interceptării acestea nu pot fi înțelese direct. În multe versiuni ale unor sisteme de operare, fișierele care conțin parolele utilizatorilor se stochează în forma criptată. De asemenea, arhivele în care se păstrează datele sau documentele cu care compania sau organizația respectivă nu mai lucrează pentru o perioadă mai mare de timp sunt criptate și abia apoi puse la păstrare. Criptarea a devenit cea mai populară metodă de protecție, atât pentru comunicații, cât și pentru datele cu caracter secret.

Pe măsura conștientizării beneficiilor aduse de utilizarea criptării, a dezavantajelor lipsei de protecție a informațiilor și a faptului că tehnologia de criptare a devenit mai accesibilă, criptarea devine o metodă atractivă de protejare a datelor, indiferent dacă este vorba de date secrete transmise prin rețea sau date obișnuite stocate în sistemul de calcul.

## Concluzie

Odată cu evoluția tehnologică din ultimii ani și datorită mediului electronic de transmitere, stocare și gestionare a informațiilor din secolul prezent, un secol al vitezei și al globalizării, se pune tot mai des problema securității informatice.

Pentru a menține un nivel de securitate individuală și socială cât mai ridicat, dat fiind faptul că produsele hardware și software evoluează constant, sunt concepții umane, cu vulnerabilități, care pot fi exploatate de anumite persoane prin contra metode sau inginerie inversă, un volum tot mai mare de date și informații necesită o protecție adecvată și un nivel de clasificare corespunzător.

Adaptarea permanentă a procesului de instruire, în ansamblul său, la particularitățile sistemelor informatice ale Alianței va determina favorabil realizarea capabilităților operaționale ale forțelor și implicit, un sistem performant de instruire, va determina o gestionare corectă, completă și protejată a informațiilor pentru apărare și a sistemelor informatice și mediilor diferite de stocare, transport, colectare și distribuire specifice.

## Bibliografie

1. Parziale L., Britt D. T., Davis Ch., Forrester J., Wei Liu, Matthews C., Rosselot N. TCP/IP Tutorial and Technical Overview. Business Machines Corporation, 2006.
2. Karygiannis T., Owens L. Wireless Network Security 802.11, Bluetooth and Handheld Devices. Computer Security Division Information Technology Laboratory National Institute of Standards and Technology, Gaithersburg, 2002.
3. Canavan J. E. Fundamentals of Network Security. Artech House, 2001.
4. Parent F. Managing Cisco Network Security: Building Rock-Solid Networks. Syngress Publishing, 2000.
5. Leidigh Ch. Fundamental Principles of Network Security. American Power Conversion, 2005.

## STUDIUL RENGHENO-STRUCTURAL A FILMELOR SUBȚIRI SB(Fe)

Igor Postolachi, UST, Moldova

Mariana Osiac, UCV, România

**Abstract.** X-ray diffraction and electron micrographic analyses showed that GaSb< Fe> eutectic composites doped with 0.1% and 0,5% Fe atoms are perfective. The density of inclusion in GaSb< Fe> composites increased about two times than undoped samples. iron-doped gallium antimony thin films at concentrations in the range (0.1÷2.0) atomic% were obtained by laser ablation.

Antimoniul de galiu (*GaSb*) se cercetează intens în ultimii ani, datorită perspectivei de a confecționa pe baza acestui semiconductor cu banda energetică îngustă ( $E_g = 0,7eV$ ) diferite dispozitive optoelectronice în diapazonul infraroșu apropiat  $\lambda=1,0\div2,5\mu m$ . Datorită poziționării în centrul diagramei  $E_g = f(a)$ , fig.1, antimoniul de galiu în ultimii ani a devenit

integrat în multe dispozitive optice [1, 2], incluzând diode emițătoare de lumină, [3] fotodetectoare, [4, 5], laserele cu diode [6, 7], fotoelemente [8] și dispozitive termoelectrice [9].

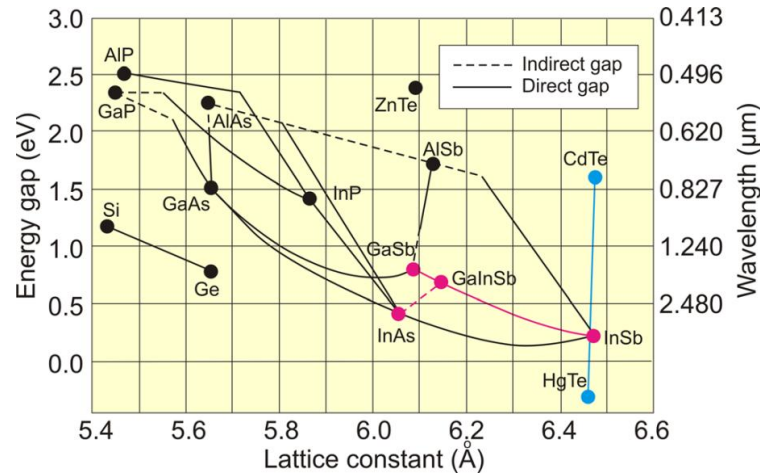


Fig. 1. Tabloul poziționării materialelor cu proprietăți de semiconductor pentru tehnica infraroșie [9].

Cercetarea intensă, în deosebi din ultimii ani a structurilor pe bază de *GaSb* este provocată de următoarele motive [10]:

- ✓ provocările percepute de fabricare pentru detectoarele tip *T2SL* (Type-II Super Lattices) a unor rețele de plan focal (FPA - focal plane arrays) cu funcționalitate ridicată la un cost rezonabil și predicțiile teoretice ale cu rata recombinării Auger mai inferioară și cu parametrii apropiați de materialul de bază pentru tehnica infraroșie pe bază de  $Hg_{1-x}Cd_xTe$ ;
- ✓ recombinarea de tip Auger cu rata inferioară probabil poate fi transformată într-un avantaj fundamental pentru *T2SL* față de  $Hg_{1-x}Cd_xTe$  în termenii unui curent de valori mai mici și a unei temperaturi de funcționare mai ridicate, în condiția ca alți parametri, cum ar fi durata timpului de viață de tipul Shockley-Read-Hall să fie egali.

Problema comportării dopanților din grupa elementelor de tranziție și grupa pământurilor rare și influența lor asupra modificării spectrului energetic al purtătorilor de sarcină în antimoniul de galiu este actuală și are un aspect cum teoretic așa și aplicativ.

Au fost obținute filme de GaSb și GaSb(Fe) depuse pe plăci de Si și Al prin metoda ablație laser. În calitate de sursă energetică a fost utilizat laserul de model Surelite II Nd:YAG (fig.2).

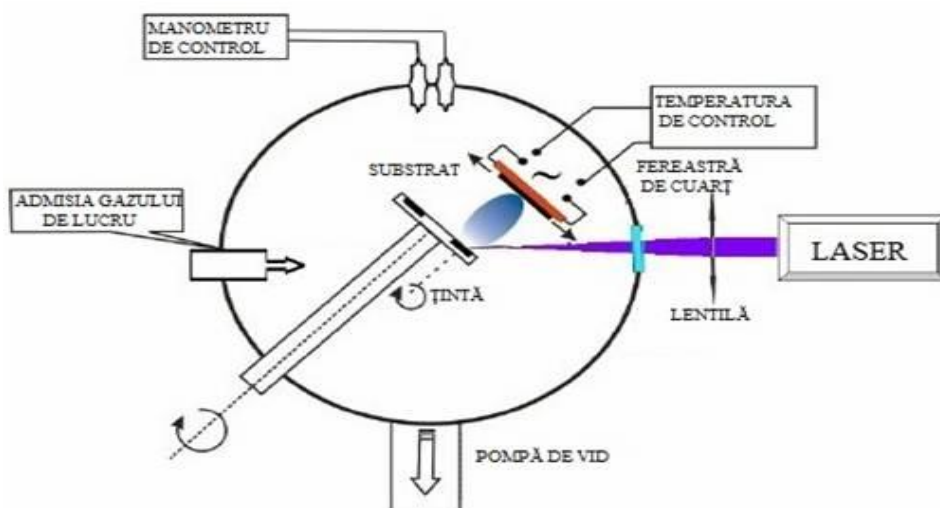


**Fig. 2.** Parametrii pentru laser Surelite II Nd:YAG:  
 Puterea  $P = 450-850$  mJ pentru lungimea de undă 1064 nm;  
 Frecvența impulsurilor 30 Hz  
 Armonice: 1064nm; 355 nm; 532nm; 266 nm

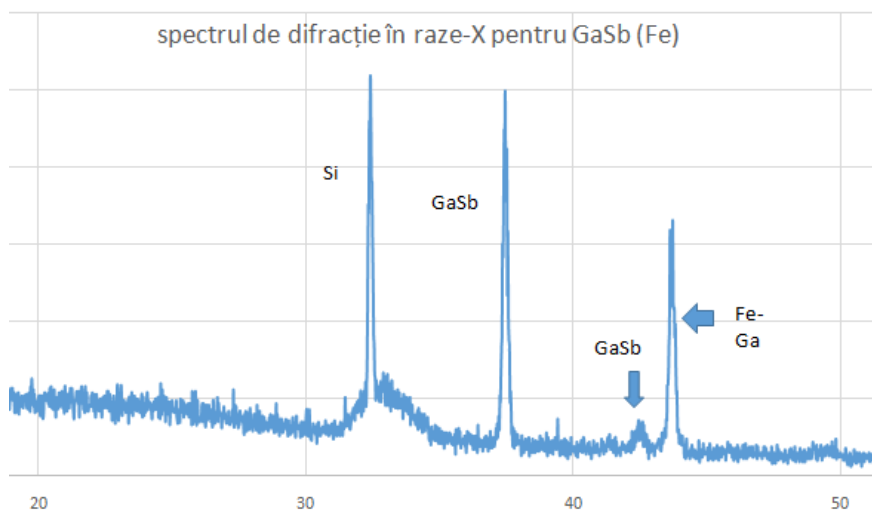
În fig. 3. este prezentată schema principală a camerei pentru obținerea filmelor de GaSb prin ablație laser. Mostrele de GaSb sau GaSb (Fe) au fost fixate pe suport și serveau ca țintă.

Radiația laser era focusată pe suprafața țintei (GaSb) cu ajutorul lentilei. Suportul împreună cu ținta se aflau în mișcare de rotație. Sub acțiunea fotonilor laser o parte din substanța țintei este evaporată și îndepărtată către suport.

În fig. 2 este prezentată spectrul de difracție a filmului de GaSb-Fe. Înregistrarea a avut loc în regiunea unghiulară  $2\theta = 20 \div 80$  grade. Distanțele dintre interplane au fost determinate cu ajutorul formulei Wolf-Bragg. Din figură se poate vedea că cel mai puternice linii de interferență corespund unghiurilor 32,50; 37,46; 42,44; 44,52 grade. Calculele arată că liniile de interferență pentru unghiurile: 37,46; 42,44; grade. corespund planurilor (210), (220), pentru antimonidul de galiu:



**Fig. 3.** Schema principială a camerei pentru obținerea filmelor subțiri de GaSb prin metoda ablație laser



## Bibliografie

1. Dutta P. S., Bhat H. L., Kumar V. J Appl Phys 81(9), 5821-5870 (1997).
2. Georgetse E., Gutzuleac L., Mikhelake A., Postolachi I., Yuldashev Sh., Kang T. Columbia International Publishing. Journal of Luminescence and Applications. Vol. 1. No.1. pp. 1-6. (2014), IF 2,367, ISSN: 0022-2313.

3. Ricker R. J., Hudson A., Provence S., Norton D. T., Olesberg J. T., Murray L. M., Prineas J. P., Boggess T. F., Ieee J. Quantum Elect 51(12), 1-6 (2015).
4. Postolachi I. American Institute of Physics. Proceedings of the physics conference TIM-08. Melville, New-York, 2009. pp.92-95.
5. Li X. C., Jiang D. W., Zhang Y., Zhao L. C. SuperlatticeMicrost 91, 238-243 (2016).
6. Merghem K., Teissier R., Aubin G., Monakhov A. M., Ramdane A., Baranov A. N. Applied Physics Letters 107(11), 2015.
7. Le H. Q., Turner G. W., Eglash S. J., Choi H. K., Coppeta D. A. Applied Physics Letters, 64(2), 152-154, 1994.
8. Hvosticov V.P. ş.a .FTP. 40 (10), 1275, 2006.
9. Aliyev M.I., Khalilova A.A., Arasly D.H., Rahimov R.N., Tanoglu M., Ozyuzer L. Strain gauges of GaSb-FeGa<sub>1,3</sub> eutectic composites. Appl. Phys.:A, 79, (8), 2075-2079, 2004.
10. Rogalski A., Martyniuk P., Kopytko M. Applied Physics Reviews 4, 031304, 2017.

**INTEGRABILITATEA DARBOUX PENTRU SISTEMELE DIFERENŢIALE  
CUBICE CE POSEDĂ TREI DREPTE INVARIANTE REALE ÎN POZIŢIE  
GENERICĂ A CĂROR MULTIPLICITATE TOTALĂ ESTE EGALĂ CU ŞASE  
ÎMPREUNĂ CU DREAPTA DE LA INFINIT**

**Vadim Repeşco**, dr., conf. univ. inter.

Catedra AMED, Universitatea de Stat din Tiraspol

**Rezumat.** Fie sistemul diferenţial cubic general  $\dot{x} = P(x, y)$ ,  $\dot{y} = Q(x, y)$ , unde  $P, Q \in \mathbb{R}[x, y]$ ,  $\max\{\deg P, \deg Q\} = 3$ ,  $GCD(P, Q) = 1$ . Conform [1], un sistem diferenţial este integrabil Darboux, dacă sistemul dat posedă un număr suficient de drepte invariante considerate cu multiplicităţile lor. În această lucrare se obţin 2 sisteme ce reprezintă formele canonice ale sistemelor diferenţiale cubice ce posedă trei drepte invariante reale în poziţie generică a căror multiplicitate totală este egală cu şase împreună cu dreapta de la infinit. Mai mult de atât, sunt calculaţi factorii lor integranţi de tip Darboux.

**Abstract.** Consider the general cubic differential system  $\dot{x} = P(x, y)$ ,  $\dot{y} = Q(x, y)$ , where  $P, Q \in \mathbb{R}[x, y]$ ,  $\max\{\deg P, \deg Q\} = 3$ ,  $GCD(P, Q) = 1$ . According to [1], a differential system is Darboux integrable if this system has sufficiently many invariant straight lines considered with their multiplicities. In this paper we obtain 2 canonical forms of cubic differential systems which possess three real invariant straight lines in generic position of total multiplicity seven including the straight line at the infinity. Moreover, we compute their Darboux integrating factors.

**Cuvinte cheie:** sistem diferenţial cubic, dreaptă invariantă, integrabilitate Darboux.

**Keywords:** cubic differential system, invariant straight line, Darboux integrability.

## Introducere

Considerăm sistemul diferenţial polinomial real de ecuaţii diferenţiale