УДК 681.322.067

В.В. Гніліцький, к.т.н., доц.
Житомирський інженерно-технологічний інститут
Ю.П. Жураковський , д.т.н., проф.
С.А. Лаптєв, аспір.
Національний технічний університет України "КПІ"

ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ

Проаналізовані властивості інформації як предмета захисту в системі автоматизованої обробки й обміну даними в сучасних умовах. Показана необхідність захисту інформації в автоматизованих системах. Наведено класифікацію засобів захисту інформації. Проаналізовані та систематизовані потенційні загрози безпеки інформації.

1. Вступ

Використання комп'ютерів і автоматизованих технологій, яке набуло поширення останнім часом, призвело до появи ряду проблем. Комп'ютери, часто об'єднані в мережі, дозволили користувачеві одержати доступ до колосальної кількості найрізноманітніших даних. Тому виникла потреба у забезпеченні безпеки інформації через наявність ризиків, пов'язаних з автоматизацією та наданням багатьом користувачам широкого доступу до конфіденційних, персональних чи інших критичних даних. Як показала практика, збільшується кількість комп'ютерних злочинів, що може призвести, у кінцевому рахунку, до підриву економіки. Тобто, стало ясно, що інформація – це ресурс, який треба захищати.

Швидка комп'ютеризація суспільства та поява нових, раніше невідомих злочинів у сфері комп'ютерної інформації довели, що правоохоронні органи не готові до адекватного протистояння й активної боротьби з цим новим соціальним явищем. Комп'ютерна злочинність стала однією з міжнародних проблем, що обумовлена створенням міжнародних інформаційних систем. Наприклад, таких, як мережа "Інтернет", що поєднує обчислювальні центри й системи багатьох країн і забезпечує обмін даними між різними центрами інформації та користувачами. У розвинутих країнах цей вид злочинності приносить великі втрати власникам і користувачам автоматизованих систем, змушує їх витрачати великі кошти на розробку та впровадження програмних, технічних та інших засобів захисту від несанкціонованого доступу до інформації, її підтасування чи знищення. Відомо, що комп'ютерні злочини щорічно приносять величезні збитки [1]. Останнім часом на Україні спостерігається стрімкий підйом злочинів, пов'язаних з втручанням у роботу автоматизованих систем. Як правило, це втручання здійснюється з метою скоєння інших, більш тяжких злочинів.

Особливо уразливими сьогодні залишаються незахищені системи зв'язку, у тому числі, обчислювальні та автоматизовані системи і мережі. Інформація, що циркулює в них, може бути незаконно змінена, вкрадена чи знищена. Останнім часом у засобах масової інформації з'явилася безліч сенсаційних повідомлень про факти злочинних впливів на автоматизовані системи обробки, збереження та передачі інформації.

У липні 1994 р. на Україні був прийнятий Закон "Про захист інформації в автоматизованих системах". В ньому були визначені основні терміни: "автоматизована система" (АС), "інформація в АС", "захист інформації", "несанкціонований доступ", "просочування інформації" та ін. Визначено, що об'єктами захисту є інформація, що знаходиться в автоматизованих системах, та власник цієї інформації.

Під втручанням у роботу АС необхідно розуміти будь-які злочинні дії, що впливають на обробку інформації в АС, тобто на всю сукупність операцій (збереження, введення, запис, перетворення, передавання, зчитування, знищення, реєстрація), що здійснюються за допомогою технічних і програмних способів, включаючи обмін через канали передачі даних. При втручанні в роботу АС відбувається її порушення, що сприяє руйнуванню процесу обробки інформації, внаслідок чого перекручується (чи знищується) сама інформація чи її носії. Під знищенням інформації розуміється її втрата, коли інформація в АС перестає існувати як для фізичних, так і для юридичних осіб, які мають право власності на неї. Втручання в роботу АС може бути й у формі впливу на канали передачі інформації, що знаходяться як між технічними засобами її обробки й збереження усередині АС, так і між окремо взятими АС, унаслідок чого інформація, що передається, знищується чи перекручується. Під перекручуванням інформації розуміємо зміну її змісту, порушення її цілісності, у тому числі, її часткове знищення. Навмисні дії, які націлені на порушення роботи автоматизованих систем, призводять до безпосереднього розкриття чи зміни даних. "Шкідницькі" програми іноді неправильно прирівнюються до комп'ютерних вірусів, тоді як віруси – тільки один із численних видів "шкідницьких" програм. Особу, яка здійснює несанкціоновану дію, з метою підвищення вразливості інформації, називають зловмисником. Дії зловмисника можна розділити на чотири основні категорії:

- переривання – припинення нормальної обробки інформації, наприклад, унаслідок руйнування обчислювальних засобів. Відзначимо, що переривання може мати серйозні наслідки навіть у тому випадку, коли сама інформація ніяким впливам не піддається;
- крадіжка, розкриття – читання чи копіювання інформації, з метою одержання даних, що можуть бути використані зловмисниками чи третьою стороною;
- модифікація (зміна) інформації;
- знищення – безповоротна зміна інформації, наприклад, стирання даних з носія.

У загальній системі забезпечення безпеки інформації виділяють такі способи захисту: фізичний, законодавчий, організаційний, програмно-технічний.

На жаль, так склалося, що підхід до класифікації інформації, з точки зору рівня вимог до її захищеності, головним чином базується на розгляді й забезпеченні тільки однієї особливості інформації – конфіденційності, а вимоги до забезпечення цілісності й доступності інформації, як правило, тільки фігурують серед загальних вимог до системи обробки цих даних. Вважається, що якщо до інформації має доступ тільки вузьке коло довірених осіб, то ймовірність її модифікації (несанкціонованого знищення) незначна. Низький рівень довіри до АС і перевага паперової інформаційної технології значно збільшують обмеженість даного підходу.

На першому етапі розвитку концепцій забезпечення безпеки даних перевага віддавалася програмним засобам захисту. Коли практика показала, що цього недостатньо, інтенсивний розвиток одержали всілякі пристрої та системи. Поступово, у міру формування системного підходу до проблеми забезпечення безпеки даних, виникла необхідність комплексного застосування методів захисту та створених на їх основі засобів і механізмів захисту [2, 3].

2. Засоби захисту інформації

На рис. 1 надана класифікація засобів захисту даних. Як випливає з нього, всі засоби захисту даних поділяють на дві основні групи: формальні та неформальні.

Формальні засоби захисту

Формальними називаються такі засоби захисту, які виконують свої функції за заздалегідь установленими процедурами без втручання людини. До формальних засобів захисту відносяться технічні й програмні засоби (рис. 1). До технічних засобів захисту відносяться всі пристрої, що призначені для захисту даних. У свою чергу, технічні засоби захисту можна розділити на фізичні й апаратні. При цьому фізичними називаються засоби захисту, що створюють фізичні перешкоди на шляху до даних, які захищаються, і не входять до складу апаратури АС, а апаратними – засоби захисту даних, що безпосередньо входять до складу апаратури АС.

Програмними називаються засоби захисту даних, що функціонують у складі програмного забезпечення АС.

Окрему групу формальних засобів складають криптографічні засоби, що реалізуються у вигляді програмних, апаратних і програмно-апаратних засобів захисту.

Фізичні засоби захисту

Фізичні засоби є дуже дорогими і не завжди дають бажані результати. Система захисту, що заснована на традиційно фізичних способах, вимагає залучення великих людських ресурсів і твердої регламентації діяльності всього персоналу, який бере участь у цьому процесі. Слабким місцем такої системи захисту є людський фактор. Отже, фізичні методи захисту не прийнятні для невеликих структур недержавного масштабу.

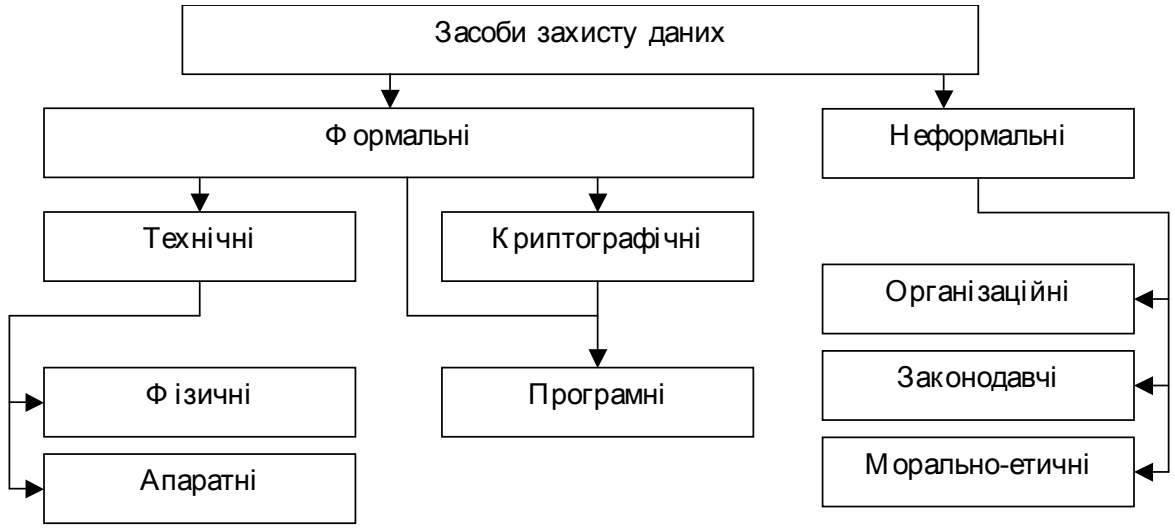

Рис. 1. Класифікація засобів захисту даних

Фізичні засоби захисту створюють перешкоди для порушників на шляху до даних, що захищаються, наприклад, на території, на якій розташовуються об'єкти АС, у приміщеннях з апаратурою, носіями даних і т. п.

Фізичні засоби захисту виконують такі основні функції [4]: охорона території та будинків; охорона внутрішніх приміщень; охорона устаткування й спостереження за ним; контроль доступу в зони, що захищаються; нейтралізація випромінювань і наведень; створення перешкод візуальному спостереженню й підслуховуванню; протипожежний захист; блокування дій порушника і т. п.

Апаратні засоби захисту

Під апаратними засобами захисту розуміють спеціальні засоби, що безпосередньо входять до складу технічного забезпечення АС і виконують функції захисту як самостійно, так і в комплексі з іншими засобами.

Апаратні засоби захисту даних можна умовно розбити на групи відповідно до типів апаратури, в якій вони використовуються. Це [4, 5]:

- засоби захисту процесора;
- засоби захисту пам'яті;
- засоби захисту терміналів;
- засоби захисту пристроїв введення–виведення;
- засоби захисту каналів зв'язку.

Коротко розглянемо зміст засобів захисту перерахованих груп апаратури.

Процесори. Однією з головних умов забезпечення безпеки даних, що обробляються, є забезпечення неможливості впливу однієї програми на процес виконання іншої і, особливо, на виконання програм ОС.

Пам'ять. Багато ЕОМ і пристроїв, що входять до складу АС, містять різні механізми захисту пам'яті для запобігання читання й модифікації даних різними користувачами.

Термінали, звичайно, містять замки для запобігання несанкціонованого включення, а також блокатори. Блокатори можуть містити пристрої ідентифікації користувача за жетоном, відбитками пальців і т. п. Для систем з високими вимогами до забезпечення безпеки даних термінали забезпечуються вбудованими схемами шифрування даних, ідентифікації термінала тощо.

Пристрої введення–виведення для вирішення задач захисту можуть містити:

- регістри адресів та ідентифікаторів;
- регістри границь виділеної пристрою пам'яті, схеми перевірки каналу введення–виведення;
- регістри контролю рівня таємності каналу зв'язку;
- схеми контролю номера каналу і т. п.

Застосування в різних системах довгих ліній зв'язку і великого числа терміналів може послужити серйозною причиною зниження рівня схоронності інформації як унаслідок несанкціонованого використання власне терміналів, так і через прослуховування ліній зв'язку.

Для забезпечення схоронності інформації у цьому випадку можуть бути використані схемні методи, специфічні програмні засоби, захисні перетворення інформації та організаційні заходи щодо захисту терміналів і ліній зв'язку, але практично єдиним засобом, що забезпечує схоронність, є захисні перетворення.

Однак і в цьому випадку необхідні спеціальні методи і пристрої, що дозволяють підвищити стійкість даних до розшифровки. Один з них – використання пристроїв передачі сторонніх повідомлень: у період, коли обмін між пристроями по каналах зв'язку не ведеться, у канал зв'язку передається стороння інформація в зашифрованому вигляді. Апаратура чи програмне забезпечення необхідні на обох кінцях лінії зв'язку: на передавальному – для формування сторонніх повідомлень, на приймальному – для розпізнавання зарезервованих символів, що відрізняють стороннє повідомлення від корисних даних.

Щоб виключити передачу даних по несанкціонованому каналу зв'язку, а також передачу даних у канал зв'язку, до якого підключився незареєстрований користувач, використовується також схема перевірки зворотного коду. До моменту передачі інформації у канал зв'язку спеціальна схема здійснює запит термінала користувача і порівнює отриману у вигляді визначеного кодового слова відповідь з наявним паролем. Тільки після встановлення відповідності паролів підготовлені дані передаються по каналу зв'язку користувачеві.

У будь-якому випадку, при створенні захищеної системи зв'язку необхідно враховувати, що стійкість може розглядатися як передбачення поводження нападаючої сторони (порушника) у плані витрат, які ця сторона повинна понести для розкриття системи захищеного зв'язку чи розкриття конкретного сеансу зв'язку. Тому витрати (і, відповідно, стійкість) на створення системи захищеного зв'язку повинні бути сумірні з передбачуваними витратами нападаючої сторони на розкриття системи. Під захистом може розумітися не обов'язково неможливість розкриття конкретного повідомлення, а утруднення для нападаючої сторони, що пов'язані з витратами засобів, часу й інших ресурсів. Утруднення, наприклад, для системи з масовим застосуванням недорогих засобів захисту можуть виявитися такими, що нападаюча сторона може відмовитися від заходів щодо розкриття. Такий рівень стійкості прийнято називати тактичним, на відміну від стратегічного, що припускає витрати нападаючої сторони, які перевищують її можливості, співвіднесені з досить тривалим інтервалом часу. Звичайно для стратегічного рівня розгляддається період часу стійкості від одиниць до десятків років.

Програмні засоби захисту

Програмними називаються засоби захисту даних, що функціонують у складі програмного забезпечення засобів і механізмів захисту даних. Вони виконують функції захисту даних самостійно чи в комплексі з іншими засобами захисту [3, 6, 7].

До програмних засобів захисту відноситься перетворення інформації. Перетворення інформації – це кодування даних. Кодування може дати позитивні результати при пасивних і активних спробах проникнення в систему, крім того, забезпечує захист даних не тільки від забороненого доступу, з метою зчитування, але і при фізичній втраті даних.

Перетворення інформації містить у собі набір оборотних логічних операцій над окремими символами запису чи над безліччю записів, що містяться в даних.

На практиці також використовується деяка послідовність перетворень, що забезпечує захист інформації користувача. Природно, що порушник може одержати ключ шляхом аналізу перехопленого кодованого повідомлення. Захисні міри, що забезпечують схоронність ключа, задаються робочим фактором перетворень, який визначається типом виконуваного кодування, статистичними характеристиками мови повідомлень, розмірами області ключа тощо. Серед інших критеріїв вибору типу захисних перетворень можна відзначити такі:

- довжина ключа. Ключ, що забезпечує захист, повинен бути також захищений. Вважається, що кращий захист забезпечується, якщо довжина ключа дорівнює повідомленню, що захищається [6];
- складність перетворень. Цей фактор визначає вартість впровадження й використання системи захисту в плані застосування додаткових технічних засобів і збільшення витрат машинного часу. При цьому істотно підвищується робочий фактор системи;
- чутливість до помилок. Помилки передачі повідомлень та збої процесора можуть виключити можливість декодування інформації.

Дамо коротку класифікацію алгоритмів шифрування:

Симетричні (із секретним єдиним ключем, одноключові, single-key):

Потокові (шифрування потоку даних):

з одноразовим чи нескінченним ключем (infinite-key cipher);

з кінцевим ключем (система Вернама – Vernam);

на основі генератора псевдовипадкових чисел (ПВЧ).

Блокові (шифрування даних поблочно):

шифри перестановки (permutation, P-блоки);

шифри заміни (підстановки, substitution, S-блоки):

моноалфавітні (код Цезаря);

поліалфавітні (шифр Відженера, циліндр Джефферсона, диск Уетстоуна, Enigma);

складені:

Lucipher (фірма IBM, США);

DES (Data Encryption Standard, США);
FEAL-1 (Fast Enciphering Algoritm, Японія);
IDEA/IPES (International Data Encryption Algorithm/Improved Proposed Encryption Standard, фірма Ascom-Tech AG, Швейцарія);
B-Crypt (фірма British Telecom, Великобританія);
ГОСТ 28147-89 (СРСР);
Skipjack (США).

Асиметричні (з відкритим ключем, public-key):
DH – Діффі–Хеллмана (Diffie, Hellman);
RSA – Райвест–Шамір–Адлемана (Rivest, Shamir, Adleman);
ElGamal (Ель-Гамаль).

Крім того, є поділ алгоритмів шифрування на власне шифри (ciphers) і коди (codes) [3]. Шифри працюють з окремими бітами, літерами, символами. Коди оперують лінгвістичними елементами (склади, слова, фрази).

Програмні засоби зовнішнього захисту включають програмні засоби забезпечення функціонування фізичних засобів: захисту території, приміщень, окремих каналів зв'язку і пристроїв АС. У наш час випускається безліч систем охоронної сигналізації, що містять мікропроцесори та ЕОМ. Програмні засоби використовуються також у пристроях упізнання особистості за різними характеристиками такими, як голос, відбитки пальців та ін. Основним методом захисту даних, що передаються по каналах зв'язку, є криптографічне закриття даних, що реалізується програмними, апаратними й програмно-апаратними засобами.

Існуючі засоби захисту даних у каналах зв'язку за принципом побудови ключової системи й системи аутентифікації можна розділити на дві групи. До першої групи віднесемо засоби, що використовують для побудови ключової системи й системи аутентифікації симетричні криптоалгоритми, до другої – асиметричні.

Симетричні алгоритми шифрування (криптографія з секретними ключами) базуються на тому, що відправник і одержувач інформації використовують той самий ключ. Цей ключ зберігається у таємниці та передається способом, що виключає його перехоплення.

В асиметричних алгоритмах шифрування (криптографія з відкритим ключем) для шифрування інформації використовують один ключ (відкритий), а для розшифровування – інший (секретний). Ці ключі різні й не можуть бути отримані один з іншого. Крім цього, використовуються такі програмні засоби:

- упізнання кореспондентів;
- перевірки рівня таємності каналу;
- перевірки адреси кореспондентів;
- перевірки ідентифікаторів кореспондентів під час обміну великими обсягами даних і т. д.

Програмні засоби внутрішнього захисту охоплюють сукупність засобів і механізмів захисту даних, що знаходяться в апаратурі АС. Їхнім основним призначенням є регулювання й контроль використання даних і ресурсів системи в жорсткій відповідності до встановлених прав доступу.

Типова схема функціонування цих програмних засобів включає такі основні етапи:

- установлення дійсності суб'єкта, який звертається до ресурсів системи;
- перевірка відповідності характеру запиту наданим повноваженням даного суб'єкта;
- ухвалення рішення відповідно до результату перевірки повноважень.

Неформальні засоби захисту

Неформальними називаються такі засоби захисту, що реалізуються в процесі діяльності людей, або регламентують цю діяльність. Неформальні засоби включають організаційні, законодавчі та морально-етичні міри й засоби.

Організаційні засоби захисту

Під організаційними засобами захисту розуміють організаційно-технічні та організаційно-правові заходи, що здійснюються в процесі створення й експлуатації АС для забезпечення безпеки даних.

Організаційні засоби захисту охоплюють усі структурні елементи АС на всіх етапах життєвого циклу мережі.

У роботах [1, 5] відзначаються деякі основні принципи організації робіт, що сприяють забезпеченню безпеки даних.

Мінімізація відомостей, доступних персоналу. Цей принцип означає, що кожен співробітник повинен знати тільки ті деталі процесу забезпечення безпеки даних, які необхідні йому для виконання своїх обов'язків.

Мінімізація зв'язків персоналу. Організація технологічного циклу збору, обробки й передачі даних, у міру можливості, повинна виключати чи мінімізувати контакти обслуговуючого персоналу.

Поділ повноважень. У системах із високими вимогами по забезпеченню безпеки даних відповідальні процедури виконуються, як правило, після підтвердження їхньої необхідності двома співробітниками.

Мінімізація доступних даних вимагає обмеження кількості даних, що можуть бути доступні персоналу й користувачам.

Дублювання контролю. Контроль найважливіших операцій не можна доручати одному співробітнику.

Ведення експлуатаційної документації має на увазі фіксацію факту передачі зміни з перерахуванням того, що й у якому стані передається.

Особливості організації забезпечення безпеки даних відбиваються в експлуатаційній документації та функціональних обов'язках персоналу, що розробляються з урахуванням мети й задачі, які стоять перед АС, і вимог по захисту даних у ній.

У системах із підвищеними вимогами до захисту вводиться спеціальна посадова особа, яка займається питаннями забезпечення безпеки даних.

Законодавчі міри захисту

Негативним наслідком інформатизації суспільства є поява так званих комп'ютерних злочинів. Поширення комп'ютерних систем, об'єднання їх у мережі розширює можливості несанкціонованого доступу до даних.

Законодавчі міри дозволяють стримувати потенційних злочинців, причому під законодавчими мірами розуміють законодавчі акти, якими регламентуються правила використання даних обмеженого доступу та встановлюються міри відповідальності за порушення цих правил.

Морально-етичні норми

До морально-етичних норм захисту відносяться всілякі норми, що традиційно склалися чи складаються в міру розвитку інформатизації суспільства. Такі норми не є обов'язковими, однак їхнє недотримання веде, як правило, до втрати авторитету, престижу людини, групи чи цілої організації. Вважається, що етичні норми впливають на персонал і користувачів.

Морально-етичні норми можуть бути неписаними й оформленими як звід правил і розпоряджень (кодексів).

3. Висновки

У даній статті проаналізовані властивості інформації як предмета захисту в системі автоматизованої обробки й обміну даними в сучасних умовах. Детально показана необхідність захисту інформації в автоматизованих системах. Наведена класифікація засобів захисту інформації. Проаналізовані та систематизовані потенційні загрози безпеки інформації. В результаті аналізу визначені: предмет, об'єкти, мета й задачі захисту.

Із засобів захисту інформації були розглянуті: формальні, до яких відносяться фізичні, апаратні та програмні; неформальні – організаційні, законодавчі й морально-етичні. Головна увага при розгляді засобів захисту інформації була приділена апаратним і програмним засобам захисту.

Показано, що захищати компоненти автоматизованих систем необхідно від усіх видів впливів: стихійних лих і аварій, збоїв та відмов технічних засобів, помилок персоналу й користувачів, помилок у програмах і від навмисних дій зловмисників.

ЛІТЕРАТУРА:

1. *Шураков В.В.* Обеспечение сохранности информации в системах обработки данных (по данным зарубежной печати). – М.: Финансы и статистика, 1985. – 224 с.
2. *Герасименко В.А.* Проблемы защиты информации в системах их обработки / Зарубежная радиоэлектроника. – 1989. – № 12. – С. 5–21.
3. *Новосельский А.* Алгоритмы шифрования. Компьютеры + программы. – 1996. – № 5. – С. 21–24.
4. *Герасименко В.А., Размахнин М.К., Родионов В.В.* Технические средства защиты информации / Зарубежная радиоэлектроника. – 1989. – № 12. – С. 22–35.
5. *Хоффман Л.Дж.* Современные методы защиты информации. – М.: Советское радио, 1980. – 264 с.
6. *Зегжда Д.П., Ивашко А.М.* Как построить защищенную информационную систему. Технология создания безопасных систем /Под научной редакцией Д.П. Зегжды и В.В. Платонова. – С.-Пб.: НПО "Мир и семья–95", ООО "Интерлайн", 1998. – 256 с.
7. Защита информации в компьютерных системах и сетях / Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин; Под. ред. В.Ф. Шаньгина. – М.: Радио и связь, 1999. – 328 с.

ГНІЛІЦЬКИЙ Віталій Васильович – кандидат технічних наук, доцент, завідувач кафедри автоматики та управління в технічних системах Житомирського інженерно-технологічного інституту.

Наукові інтереси:

– теорія інформації;
– захист інформації та комп'ютерна криптографія.

ЖУРАКОВСЬКИЙ Юрій Павлович – доктор технічних наук, професор кафедри АУТС Національного технічного університету України "Київський політехнічний інститут".
Наукові інтереси:
– теорія інформації;
– кодування та захист інформації.

ЛАПТЄВ Сергій Анатолійович – аспірант Національного технічного університету України "Київський політехнічний інститут".
Наукові інтереси:
– обробка інформації;
– програмування та криптографія.

Подано 25.09.2000