УДК 004.056.5(045)

Журиленко Б.Є. Математична модель вірогідної надійності комплексу технічного захисту інформації
Анотація. *В даній роботі запропонована математична модель вірогідної надійності комплексу технічного захисту інформації (КТЗІ). Побудова моделі ґрунтується на основних початкових даних властивих захисту. Модель надійності КТЗІ орієнтована на вірогідності зломів кожного захисту в часі або всього комплексу і надалі дозволить порівняти розрахункові результати з реальними даними зломів і захищеності.*
Ключові слова: *захист інформації, надійність, вірогідність злому, комплекс технічного захисту інформації.*

Zhurilenko B.E. Mathematical model of reliable reliability for complex of technical information security
Abstract. *In the given work the mathematical model of probabilistic reliability of complex of technical information security is offered. Construction of model is based on master initial data of inherent to defence. The model of the complex of technical information security reliability is oriented on probability of breaking of every defence in time or all complex in and will in future allow to compare computation results to the real data of breaking and protected in.*
Keywords: *information security, reliability, probability of breaking in, complex of technical information security.*

Отримано *28 вересня 2012 року* , затверджено редколегією *27 листопада 2012 року*
(рецензент д.т.н., професор Г.Ф. Конахович)

АНАЛІЗ ІСНУЮЧИХ ШАБЛОНІВ СИСТЕМ АВТЕНТИФІКАЦІЇ В ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИХ СИСТЕМАХ ТА МЕРЕЖАХ

Анна Чунарьова, Андрій Чунарьов

Національний авіаційний університет

ЧУНАРЬОВА Анна Вадимівна, к.т.н., доцент

Рік та місце народження: 1987 рік, м. Вентспілс, Латвія.
Освіта: Національний авіаційний університет, 2009 рік.
Посада: доцент кафедри комп'ютеризованих систем захисту інформації кафедри з 2012 року.
Наукові інтереси: інформаційна безпека, телекомунікації.
Публікації: 63 наукові публікації, серед яких наукові статті, патенти на корисні моделі та навчально-методичні роботи.
E-mail: chunariova@gmail.com

ЧУНАРЬОВ Андрій Вадимович

Рік та місце народження: 1992 рік, м. Вентспілс, Латвія.
Освіта: Національний авіаційний університет
Посада: студент 4 курсу кафедри комп'ютеризованих систем захисту інформації кафедри з 2009 року.
Наукові інтереси: інформаційна безпека, телекомунікації.
Публікації: 42 наукові публікації, серед яких наукові статті та патенти на корисні моделі.
E-mail: chunariov@ukr.net

Анотація. *У даній статті проведено аналіз шаблонів автентифікації в сучасних інформаційно-комунікаційних системах та мережах. В результаті проведено аналізу виділені переваги та недоліки застосування існуючих шаблонів для забезпечення надійного захисту. Виділені найбільш ефективні з точки зору розмежування та контролю доступу до інформаційних ресурсів.*

Ключові слова: *захист інформації, автентифікація, верифікатор, інформаційно-комунікаційна система та мережа, система захисту.*

Актуальність. На сьогодні розмежування доступу в інформаційно-комунікаційних системах та мережах (ІКСМ) полягає в розділенні і організації доступу до інформації користувачів відповідно до їх

функціональних обов'язків і повноважень. Задача такого розмежування доступу до інформації: скорочення кількості користувачів, що не мають до неї відношення при виконанні своїх функцій, тобто захист інформації від порушника серед законних користувачів. Розмежування доступу користувачів ІКСМ може здійснюватися за наступними параметрами: виглядом, характером, призначенням, ступенем важливості і секретності інформації; способами її обробки: обчислення, запис, внесення змін, виконання команди; умовним номером терміналу; часом обробки та ін.

Постановка задачі. При проектуванні ІКСМ на її базі проводяться: розробка і реалізація функціональних задач по розмежуванню і контролю доступу до апаратури та інформації, як в рамках інформаційної системи в цілому, так і до відокремлених інформаційних ресурсів; розробка апаратних засобів ідентифікації та автентифікації користувачів та ресурсів системи; розробка програмних засобів контролю і управління розмежування доступу; розробка окремої експлуатаційної документації на засоби ідентифікації, автентифікації, розмежування і контролю доступу.

Метою даної статті являється дослідження та аналіз сучасних шаблонів автентифікації.

Аналіз існуючих шаблонів автентифікації в сучасних ІКСМ. Автентифікація являє собою процедуру перевірки дійсності ідентифікаторів. У процесі ідентифікації та автентифікації користувач або програма (претендент) запитує доступ у системи (верифікатора). Спочатку здійснюється ідентифікація. Верифікатор жадає від претендента пред'явити деякий ідентифікатор і перевіряє приналежність пред'явленого ідентифікатора, безлічі зареєстрованих у системі. У випадку коректності ідентифікатора, верифікатор виконує процедуру автентифікації (наприклад, запитує пароль), щоб переконатися, що претендент є саме тим, за кого себе видає. Допуск претендента в систему дозволяється тільки у випадку успішного завершення процедури автентифікації. У більшості систем встановлюється ще деяке граничне значення для числа спроб пред'явлення некоректного ідентифікатора і пароля, при перевищенні якого, всі подальші спроби доступу даного претендента до системи блокуються [1].

На даний час виділяють чотири відмінні шаблони систем автентифікації: локальна автентифікація, пряма автентифікація, непряма автентифікація, автономна автентифікація.

На практиці така класифікація може дотримуватись не завжди. Наприклад, існують багаторівневі системи безпеки, які можуть використовувати не один, а два або навіть більше шаблони систем автентифікації.

- Локальна автентифікація, яку можна бачити в переносних або окремо розташованих настільних системах. Вся система, включаючи механізм аутентіфікації та управління доступом, розміщується всередині одного фізичного периметра безпеки. Власник системи або користувач ведуть і оновлюють базу автентифікаційних даних всередині цього периметру.

- Пряма автентифікація, яку можна бачити в старих серверних системах, що стоять в ІКСМ, і в системах з розподілом часу. Системою можуть колективно користуватися віддаленим чином багато різних користувачів. Механізми автентифікації і контролю доступом системи як і раніше розміщуються всередині одного фізичного периметра. Власник веде і підтримує актуальною базу автентифікаційних даних всередині кожної системи.

- Непряма автентифікація, яку можна бачити в сучасних мережевих серверних системах і яка може бути реалізована через протоколи RADIUS, Kerberos і протокол реєстрації в домені ОС Windows. Система містить кілька точок обслуговування, які вимагають управління доступом і можуть розміщуватися в різних місцях. При необхідності користувачі звертаються до служб системи віддаленим чином. Власник веде і підтримує актуальною одну базу автентифікаційних даних для всієї системи.

- Автономна автентифікація, яку можна бачити в системах з інфраструктурою відкритих ключів, що містять численні автономні компоненти, які здатні приймати точні рішення по управлінню доступом навіть у тому випадку, коли вони не можуть зв'язуватися з іншими системами для отримання авторитетних рішень про автентифікації . Власник погоджується з ризиком того, що такі рішення можуть іноді прийматися з використанням застарілих даних з управління доступом або аутентіфікації, а отже, можуть давати неправильні результати.

Ці шаблони в загальному діляться на дві категорії: призначені для окремих автономних комп'ютерів і для віддаленого доступу. Як очевидно, локальна модель пов'язана з індивідуальним пристроєм. Моделі прямої та непрямої автентифікації представляють собою різні стратегії для реалізації віддаленого доступу. Модель автономної автентифікації забезпечує спосіб застосування деяких адміністративних функцій віддаленої автентифікації в системах, які не завжди можуть встановити віддалене з'єднання.

Фізичний захист є фундаментом будь-якої системи комп'ютерної безпеки. В системах автентифікації фізичний захист забезпечує цілісність механізму прийняття рішень і захищає базовий секрет. У плані фізичного захисту є два аспекти: захист програмного забезпечення і захист апаратного забезпечення. Перший випадок стосується програмного забезпечення, що виконується на звичайному готовому комп'ютерному обладнанні, яке не має зовсім або має слабкі механізми захисту від крадіжки. Останній випадок стосується апаратних пристроїв, що використовуються чужими або іншими потенційно ненадійними людьми: ці пристрої часто побудовані з урахуванням стійкості до крадіжок. Ці два випадки сходяться в проблемі захисту окремих робочих станцій чи переносних комп'ютерів, які можуть бути предметом атаки. Істотним питанням є

ідентифікація периметра безпеки пристрою або системи. Механізм прийняття рішень і всі конфіденційні дані повинні розміщуватися всередині цього периметру. Єдиними людьми, які можуть проникати всередину периметра, повинні бути адміністратори, на-значення для виконання цієї ролі власником системи. На механізм аутен-тіфікаціі можна покладатися тільки до тих пір, поки його периметр безпеки можуть перетинати тільки люди, що заслуговують довіри.

Далі розглянемо особливості кожного шаблону аутентифікації. Перший типовий шаблон – локальна автентифікації – охоплює найпростіші ситуації, коли люди працюють з системою безпосередньо, а не віддалено. Очевидні приклади включають портативні або кишенькові пристрої, хоча сюди ж можна віднести і автономні робочі станції.

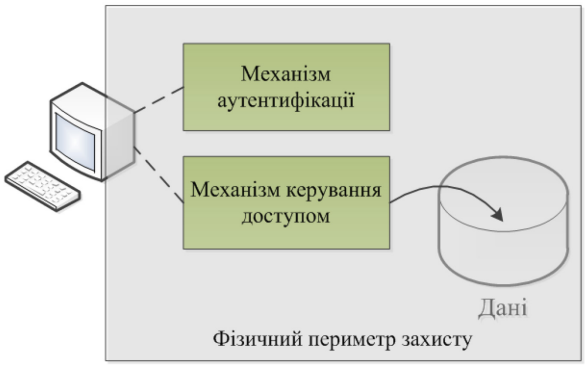

Рис. 1. Модель локальної автентифікації

Суть шаблону локальної автентифікації (рис.1) полягає в тому, що весь механізм автентифікації і управління доступом розміщується всередині одного периметра безпеки. Люди користуються комп'ютером або іншою захищеною системою через інтерфейс, який безпосередньо міститься в периметрі безпеки. Користувачі не зламують периметр, але введена ними інформація проходить через нього всередину, а виданий комп'ютером результат виходить через нього назад. Система автентифікації працює правильно тільки до ти, доки атакуюча сторона не зламає фізичний периметр безпеки.

Прикладом шаблону локальної автентифікації є переносні комп’ютери. Багато таких комп'ютерів підтримують функцію парольного замка: система не буде завантажуватися до тих пір, поки користувач не надасть правильний пароль. Хоча замок і забезпечує певний захист від несанкціонованого використання, він не зупинить зломщика, який отримає фізичне володіння комп'ютером. Рішучий зловмисник зазвичай швидко розкриває комп'ютер (зламуючи його фізичний периметр безпеки) і витягує дані безпосередньо з жорсткого диска.

У цій моделі вся система цілком розміщується всередині одного фізичного периметра безпеки. Люди вводять базові секрети або інші відмінні характеристики безпосередньо в систему. Оброблювані системою дані повністю знаходяться всередині. Приклади включають автономні робочі станції і персональні пристрої [2].

Якщо розробник системи довіряє фізичному периметру безпеки, то це значно спрощує її конструкцію і роботу. Користувачі можуть використовувати легкі для запам'ятовування паролі або навіть персональні ідентифікаційні номери (PIN-коди), так як атакуюча сторона буде прив'язана до інтерактивного вгадування пароля методом проб і помилок, як до єдиного доступного режиму атаки.

Якщо зловмисники не можуть зламати периметр, то вони й не можуть витягти паролі, що зберігаються в системі, в зашифрованому вигляді чи ні. Дійсно, надійний периметр виключає необхідність хешування паролів або шифрування в якій-небудь іншій формі. Зручність використання системи можна збільшити, реалізувавши в якості методу автентифікації біометрію. Хоча активна розвідка і відтворення являють собою основний ризик для біометричних систем, надійний фізичний периметр безпеки виключає можливість проведення таких атак. На практиці, звичайно, дуже складно гарантувати неприступність фізичного периметра.

Для багатьох підприємств основним недоліком локальної автентифікації є її адміністрування. Кожен пристрій являє собою окремий пункт обслуговування, який повинен адмініструватись індивідуально. Якщо двом людям необхідно мати доступ до одного захищеного комп'ютера, то обом необхідні автентифікаційні дані, наприклад колективний пароль.

Типовий шаблон прямої автентифікації в підсумку дає найпростішу архітектуру системи автентифікації віддалених користувачів. Схема працює найкраще, якщо кожен власник забезпечує наявність єдиної точки обслуговування або якщо кожна точка обслуговування має окреме співтовариство користувачів. Зазвичай власник кожної точки обслуговування знає заздалегідь, кому слід дозволити їм користуватися.

Суть моделі прямої автентифікації (див. рис. 2) полягає в тому, що обчислювальні служби розміщуються в одному фізично захищеному місці, тоді як клієнти не обов'язково захищені.

Цей шаблон називається "прямим", оскільки точка обслуговування сама приймає рішення про автентифікації. Механізм автентифікації, механізми управління доступом і самі служби знаходяться в одному пристрої. Адміністратори підтримують базу даних авторизованих користувачів в кожній системі. Зміна в базі даних користувачів має миттєвий ефект, якщо хтось намагається увійти в систему, вона звертається до своєї власної бази даних користувачів. Очевидним недоліком прямої моделі є недостатня стійкість до збоїв, оскільки все централізовано.

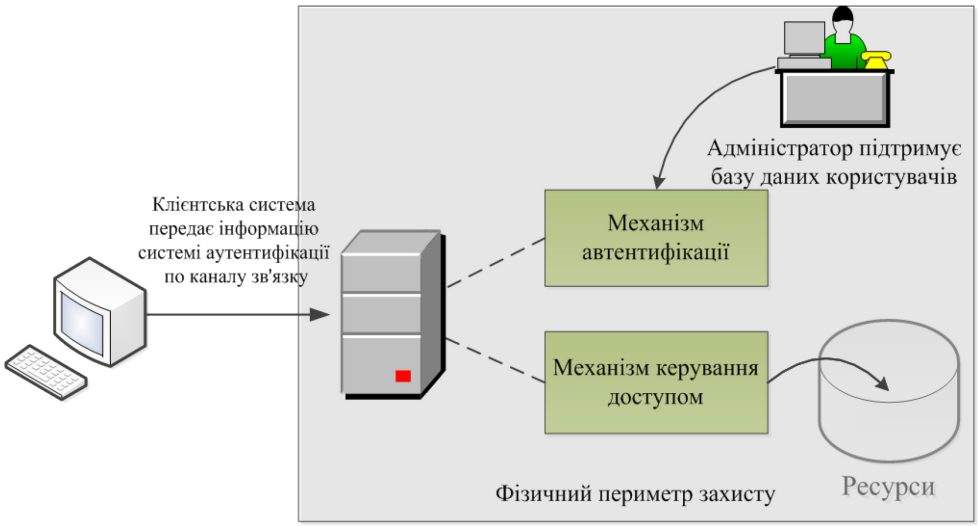

Рис. 2 Розгортання системи прямої автентифікації

Так як користувачам не обов'язково взаємодіяти з системою із захищеного місця, то зловмисники можуть вибрати в якості своєї мішені віддалені користувацькі робочі станції або їх лінії зв'язку. Це робить біометричні методи недоцільними: зловмисник може перехопити видалені біометричні показники авторизованого користувача і згодом відтворити їх, видавши себе за цього користувача. Аналогічні проблеми притаманні і для секретних паролів багаторазового використання.

Через ризик активної розвідки і відтворення системи, побудовані на основі цього шаблону, зазвичай вимагають криптографічного захисту. Це необов'язково шифрування всього трафіку; зашифрованих паролів може бути достатньо для забезпечення автентифікації відповідного рівня. Хоча такі системи можуть використовувати шифрування з відкритим або секретним ключем, в більшості продуктів цього типу використовується шифрування з секретним ключем. Рішення наоснові шаблону прямої автентифікації працюють краще за все в тому випадку, коли власник управляє однією системою або групою систем з незалежними користувачами.

Отже, відповідно до цієї моделі люди не використовують систему безпосередньо. Вони використовують систему, вводячи ідентифікуючі дані через віддаленого клієнта. Інформація надсилається, часто в зашифрованому вигляді, в базу даних авторизованих користувачів системи. Позитивний результат порівняння призводить до наділення правом доступу; механізми автентифікації і управління доступом розміщуються в одному пристрої.

Рішення на основі непрямої автентифікації дозволяють справлятися з проблеми масштабованості на обчислювальних центрах, у яких одна група користувачів, але кілька точок обслуговування. Навіть на тій площині, де всього два сервери, буде важко підтримувати сумісність двох окремих баз даних аутентифікації .

У разі використання непрямої моделі механізм автентифікації розміщується в стороні від інших серверів системи, які зв'язуються з ним, коли користувач запитує доступ. Подібне використання окремого автентифікаційного сервера, який вимагає виконання тільки одного оновлення даних для кожного користувача, на практиці здійснюється прозорим чином. Якщо інші проектні шаблони передбачають об'єднання механізмів автентифікації і управління доступом, то шаблон непрямий автентифікації (рис.3) переміщає механізм автентифікації з точки обслуговування в окремий автентифікаційний сервер. Всі інші компоненти надають послуги або управляють доступом до ресурсів, але не приймають рішень про автентифікації. Замість цього вони автентифікують людей непрямим чином, зв'язуючись з автентифікаційним сервером кожного разу, коли хтось намагається зареєструватися в системі.

Автономна автентифікації – це реалізація призначена для вирішення внутрішніх суперечностей, властивих розподіленій автентифікації: власник не може довіряти кожному пристрою, що потребує автентифікації. Деякі додатки настільки великі або є настільки розподіленими, що вони не можуть покладатися на централізований сервер в плані автентифікації в реальному часі. Але тим не менш власник хоче зберегти централізоване управління автентифікацією.

Рішення на основі моделі автономної автентифікації об'єднують особливості перших трьох моделей. Як і у випадку реалізації локального підходу, автентифікація може виконуватися на автономній системі без створення мережевого з'єднання реального часу. Як і в рішеннях на основі локального або прямого підходу, механізм автентифікації розміщується на тому ж пристрої, що і механізм управління доступом. І подібно непрямим рішенням власник може підтримувати один централізований список авторизованих користувачів.

Рис. 3. Непряма автентифікація

Прикладом реалізації автономної аутентифікації є інфраструктура відкритих ключів. Інфраструктура відкритих ключів реалізує автономні рішення шляхом використання відносно невеликої кількості заданих відкритих ключів для підтвердження автентифікаційних даних окремих користувачів або інших об'єктів. Задані ключі належать органам сертифікації, які видають сертифікати відкритого ключа, що містять автентифікаційні дані для користувачів або інших об'єктів. Автентифікація здійснюється в два етапи. Наприклад, якщо користувач хоче автентифікувати свій банківський сервер, то спочатку його робоча станція отримує сертифікат відкритого ключа банку і потім автентифікує його за допомогою заданого відкритого ключа. Другий крок полягає у використанні відкритого ключа із сертифікатом банку, як частина іншого протоколу, наприклад протоколу безпечних з'єднань Secure Sockets Layer (SSL), для автентифікації банку в якості основного власника секретного ключа, який математично пов'язаний з відкритим ключем сертифікату.

Цікавою особливістю рішень на основі автономної моделі є те, що власник не повинен створювати, підтримувати й адмініструвати записи про користувачів за допомогою інтерактивної доступної системи. Програмне забезпечення управління видачею сертифікатів, може працювати автономно і пересилати сертифікати у відкритий каталог за допомогою змінного носія. Зловмисники не можуть проникнути безпосередньо в механізм реєстрації, оскільки він недоступний в інтерактивному режимі [3].

Як і у випадку рішень на основі моделей з прямою і непрямою автентифікацією, автономна автентифікація не може використовувати біометрії в чистому вигляді.

Іншою важливою особливістю автономної автентифікації є її стійкість до відмов. Отримуючи копію відповідного сертифіката, пристрій автентифікації може автентифікувати будь-який об'єкт. Пристрій може забезпечити гарантований доступ до необхідних сертифікатів шляхом пошуку в різних каталогах, підтримуючи свій локальний кеш сертифікатів або витягуючи сертифікати з того об'єкта, який автентифіковано.

У табл. 1 зведені найбільш загальні риси чотирьох шаблонів.

У першому рядку показується частина системи, яка повинна бути фізично захищена власником щоб уникнути поширених помилок автентифікації. У другому рядку вказуються типи алгоритмів шифрування, що вимагаються для рішень відповідно до кожного з шаблонів.У третьому рядку проводиться порівняння стійкості до відмов різних шаблонів. Слово "низька" означає, що шаблон має точку критичної відмови.

Практична реалізація рішень на основі непрямої і автономної моделі як правило важче, ніж реалізація рішень на основі локальної або прямої моделі. Що стосується стійкості до відмов, то непряме рішення може забезпечувати високу стійкість до відмов, якщо практична реалізація передбачає наявність резервного автенти-фікаційного сервера.

Таблиця 1. Порівняльна характеристика шаблонів систем автентифікації

Шаблон автентифікації / *Власти-вість захисту*	*Локальний*	*Прямий*	*Непрямий*	*Автономний*
Частини системи, потребують захисту	Вся система	Тільки точки обслуговування	Тільки аутентіфікаційні сервери	Тільки органи сертифікації
Тип використовуваного шифрування	Не використовується	Секретний або відкритий ключ	Секретний або відкритий ключ	Тільки відкритий ключ
Стійкість до відмов	Низька	Низька	Висока / низька	Висока

Висновки

Проведені дослідження показали, що для сучасних ІКСМ найоптимальнішим варіантом буде використання шаблону непрямої системи автентифікації. Роль автентифікаційного сервера, що приймає запити на автентифікацію від інших серверів повинен відігравати сервер бази даних. На сервері бази даних повинна підтримуватись єдина актуальна база особистих даних користувачів, що спрощує процес адміністрування. Комплекс засобів захисту ІКСМ для забезпечення надійного захисту повинен розміщуватися на сервері бази даних, але при цьому за рахунок відповідних клієнтських додатків охоплювати всі комп'ютери робочих груп, адміністраторів та керівництва, а також всі сервери, що містяться в автоматизованій системі.

Література

[1] Теоретические основы компьютерной безопасности. Учебное пособие для вузов / П.Н. Девянин, О.О. Михальский, Д.И. Правиков. – М.: Радио и связь, 2010. – 192 с.

[2] Богуш В.М., Довидьков О.А. Теоретичні основи захищених інформаційних технологій. – К.: ДУІКТ, 2009. – 414 с.

[3] Белов Е.Б. Основы информационной безопасности. Учебное пособие для вузов / Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. – М.: Горячая линия – Телеком, 2006. – 544 с.

УДК 004.056.53 (045)

Чунарева А.В., Чунарев А.В. Анализ существующих шаблонов систем аутентификации в информационно-коммуникационных системах и сетях

Аннотация. *В данной статье проведен анализ шаблонов аутентификации в современных информационно-коммуникационных системах и сетях. В результате проведения анализа выделены преимущества и недостатки применения существующих шаблонов для обеспечения надежной защиты. Выделены наиболее эффективные с точки зрения разграничения и контроля доступа к информационным ресурсам.*

Ключевые слова: *защита информации, аутентификация, верификатор, информационно-коммуникационная система и сеть, система защиты.*

Chunariova A.V., Chunariov A.V. Analysis of existing authentication systems of information and communication systems and networks

Abstract. *This article analyzes patterns of authentication in modern information and communication systems and networks. As a result, the analysis highlighted the advantages and disadvantages of the existing templates to provide protection. Select the most efficient in terms of differentiation and control of access to information resources.*

Keywords: *information security, authentication, the verifier, information and communication system and network security system.*

Отримано *13 вересня 2012 року,* затверджено редколегією *8 листопада 2012 року*
(рецензент д.т.н., професор О.К. Юдін)

СИСТЕМА АНАЛІЗУ ТА ОЦІНКИ РІВНЯ ЗАХИЩЕНОСТІ ДЕРЖАВНИХ ІНФОРМАЦІЙНИХ РЕСУРСІВ ВІД СОЦІОТЕХНІЧНИХ АТАК

Дарина Горніцька, Марія Захарова, Андрій Кладочний

Національний авіаційний університет

ГОРНІЦЬКА Дарина Анатоліївна

Рік та місце народження: 1985 рік, м. Київ, Україна.
Освіта: Національний авіаційний університет, 2007 рік.
Посада: аспірант Національного авіаційного університету.
Наукові інтереси: інформаційна безпека, соціотехнічні атаки.
Публікації: більше 20 наукових публікацій, серед яких наукові статті та патенти на винаходи.
E-mail: darja85@ukr.net