УДК 004.056.55

ЗАХИСТ ДАНИХ ЗАСОБОМ ЦИФРОВОГО ПІДПИСУ

Плотніков В. М., Борцова Ю. В.

DOI:

Анотація.

У цей час багато підприємств використовують ті або інші методи безпаперової обробки й обміну документами. Використання подібних систем дозволяє значно скоротити час, затрачуваний на оформлення угоди й обмін документацією, удосконалити й зменшити кошти на процедуру підготовки, доставки, обліку й зберігання документів, побудувати корпоративну систему обміну документами. Однак при переході на електронний документообіг встає питання авторства документа, вірогідності й захисту від перекручувань.

Найбільш зручним засобом захисту електронних документів від перекручувань, що дозволяють при цьому однозначно ідентифікувати відправника, повідомлення, є електронний цифровий підпис (ЕЦП). Отже, що ж таке електронний цифровий підпис? Закон дає наступне визначення даного терміна: «електронний цифровий підпис - реквізит електронного документа, призначений для захисту даного електронного документа від підробки, отриманий у результаті криптографічного перетворення інформації з використанням закритого ключа електронного цифрового підпису й що дозволяє ідентифікувати власника сертифіката ключа підпису, а також установити відсутність перекручування інформації в електронному документі». Із цього визначення видно, що ЕЦП формується за допомогою спеціальних математичних алгоритмів на основі властиво документа й когось «закритого ключа», що дозволяє однозначно ідентифікувати відправника повідомлення.

Abstract.

At this time many enterprises use these or those methods of paperless processing and an exchange of documents. Use of similar systems allows to reduce considerably time spent for registration of the agreement and an exchange by the documentation, to improve and reduce the price of procedure of preparation, delivery, the account and storage of documents, to construct corporate system of an exchange of documents. However at transition to electronic document circulation there is a question of authorship of the document, reliability and protection from fakes.

The most convenient means of protection of electronic documents from fakes which allow to identify unequivocally thus of the sender, the message, is the electronic digital signature (EDS). So, what such the electronic digital signature? The law defines the following of the given term: « The electronic digital signature - the requisite of the electronic document intended for protection of the given electronic document from a fake, received as a result of cryptographic transformation of the information with use of the closed key of the electronic digital signature also that allows to identify the owner of the certificate of a key of the signature and also to establish absence fakes information in the electronic document ». From this definition it is visible, that EDS it is formed by means of special mathematical algorithms on the basis of it is peculiar the document and someone « the closed key » that allows to identify unequivocally the sender of the message. We shall consider more in detail the mechanism of functioning of systems EDS.

Ключові слова: електронний документ, безпаперовий документообіг, захист інформації, електронний цифровий підпис, асиметричні криптографічні алгоритми, сертифікат, таємний ключ, відкритий ключ.

Keywords: electronic document, paperless document management, information security, electronic digital signature, asymmetric cryptographic algorithms, certificate, secret key, public key.

Вступ

Електронний цифровий підпис функціонує на основі криптоалгоритмів з асиметричними (відкритими) ключами й інфраструктури відкритих ключів. Проблема традиційних алгоритмів шифрування із симетричними ключами полягає в тім, що шифрування й дешифрування відбувається за допомогою того самого ключа. У зв'язку із цим виникає питання про обмін ключами. Для того, щоб зробити захищений обмін інформацією, користувачам необхідно обмінятися ключами, при чому використовувати для цього обміну альтернативні засоби передачі інформації, оскільки при обміні нешифрованою інформацією з електронної пошти висока ймовірність дискредитації ключа. Ідеальним, з погляду безпеки, варіантом представляється особистий обмін ключовими носіями, однак він є найбільш ресурсномістким. У криптосистемах на основі асиметричних ключів для шифрування й дешифрування використовується пара ключів - секретний і публічний ключі, унікальні для кожного користувача, і цифровий

сертифікат. Цифровий сертифікат являє собою розширення відкритого ключа, що включає не тільки сам ключ, але й додаткову інформацію, що описує приналежність ключа, час використання, доступні криптосистеми, назва центра, що засвідчує, і т.д. Для реалізації подібної взаємодії використовуються спеціальні структури, що засвідчують центри. Їхня основна функція - поширення публічних і секретних ключів користувачів, а також верифікація сертифікатів. центри, Що Засвідчують, можуть поєднуватися в ланцюжки. Вищестоящий (кореневий) центр, що засвідчує, може видати сертифікат і права на видачу ключів нижчестоящому центру. Той, у свою чергу, може видати права ще іншому нижчестоящому центру й так далі, при чому, сертифікат, виданий одним із центрів, може бути верифицирован кожним із серверів у ланцюжку1 . У такий спосіб існує можливість установити центр поширення секретних ключів у безпосередній близькості від користувача, що вирішує проблему дискредитації ключа при передачі по мережах зв'язку. У випадку з ЄЦП процес обміну повідомленням виглядає в такий спосіб:

1. відправник одержує в центра, що засвідчує, секретний ключ;
2. використовуючи цей ключ, формує електронний цифровий підпис і відправляє лист;
3. одержувач за допомогою публічного (загальнодоступного) ключа й цифрового сертифіката, отриманого в центра, що засвідчує, установлює авторство документа й відсутність перекручувань.

Цифровий підпис забезпечує:

1. Посвідчення джерела документа. Залежно від деталей визначення документа можуть бути підписані такі поля, як «автор», «внесені зміни», «мітка часу» і т.д.
2. Захист від змін документа. При будь-якій випадковій або навмисній зміні документа (або підпису) зміниться геш, отже, підпис стане недійсної.
3. Неможливість відмови від авторства. Тому що створити коректний підпис можна лише, знаючи закритий ключ, а він відомий тільки власникові, то власник не може відмовитися від свого підпису під документом.

При використанні надійної геш-функції, вичислительно складно створити підроблений документ із таким же гешем, як у справжнього. Однак, ці погрози можуть реалізуватися через слабості конкретних алгоритмів гешировання, підпису, або помилок у їхніх реалізаціях.

Проте, можливі ще такі погрози системам цифрового підпису:

1. Зловмисник, викравший закритий ключ, може підписати будь-який документ від імені власника ключа.
2. Зловмисник може обманом змусити власника підписати який-небудь документ, наприклад використовуючи протокол сліпого підпису.
3. Зловмисник може підмінити відкритий ключ власника (див. керування ключами) на свій власний, видаючи себе за нього.

Електронний цифровий підпис є найбільш перспективним і широко використовуваним у світі способом захисту електронних документів від підробки й забезпечує високу вірогідність повідомлення. Закони дають можливість використання систем ЕЦП для обміну фінансовими й іншого критичними для діловодства документами.

Алгоритми шифрування можна розділити на два класи - симетричні й асиметричні.

Симетричні алгоритми шифрування

У симетричних алгоритмах для зашифрування й расшифрованія інформації використовується той самий криптографічний ключ. Щоб забезпечити взаємодія з будь-яким абонентом Мережі, у кожного учасника повинне бути сховище масиву секретних криптографічних ключів. Крім того, необхідно вирішити проблему централізованої генерації ключової інформації й забезпечити її безпечну доставку до всіх учасників.

Асиметричні алгоритми шифрування

В асиметричних криптографічних алгоритмах використовується пара математично взаємозалежних ключів, один із яких не є секретним і може бути розміщений у довіднику відкритих ключів . Якщо абонентові А необхідно направити конфіденційне повідомлення абонентові Б, він вибирає в довіднику відкритий ключ абонента Б и використовує його для шифрування документа. Для його расшифрованія абонент Б використовує свій секретний ключ. Таким чином, будь-який абонент Мережі може зашифрувати повідомлення, що направляється іншому абонентові, а розшифрувати його зможе тільки власник відповідного секретного ключа. Основний недолік - низька швидкодія: за деякими оцінками, асиметричні алгоритми в 100 - 1000 разів повільніше симетричних. На практиці найчастіше використовують комбіновані схеми. Абонент А сам генерує деякий випадковий ключ для симетричного алгоритму й з використанням асиметричного алгоритму на відкритому ключі абонента Б зашифровує його й передає адресатові. Одержавши зашифрований ключ, абонент Б розшифровує його з використанням свого секретного ключа. У результаті абоненти А и Б одержують унікальний ключ симетричного алгоритму, що і застосовується для шифрування властиво переданих даних. При наступній взаємодії процес повторюється, забезпечуючи кожний сеанс зв'язку різними ключами. Тому що асиметричний алгоритм застосовується для обробки невеликого обсягу інформації - тільки ключа, час на шифрування в цілому істотно не збільшується. Ассиметричні алгоритми шифрування

Розвиток основних типів криптографічних протоколів (ключовий обмін, електронно-цифровий підпис (ЕЦП), аутентификация й ін) було б неможливо без створення відкритих ключів і побудованих на їхній основі ассиметричних протоколів шифрування.

Основна ідея асиметричних криптоалгоритмов полягає в тому, що для шифрування повідомлення використовується один ключ, а при дешифруванні - іншої. Крім того, процедура шифрування обрана так, що вона необоротна навіть по відомому ключі шифрування - це друга необхідна умова асиметричної криптографії. Тобто, знаючи ключ шифрування й зашифрований текст, неможливо відновити вихідне повідомлення - прочитати його

можна тільки за допомогою другого ключа - ключа дешифрування. У цілому система переписки при використанні асиметричного шифрування виглядає в такий спосіб. Для кожного з N абонентів, ведучих переписку, обрана своя пара ключів : "відкритий" E_j і "закритий" D_j, де j – номер абонента. Всі відкриті ключі відомі всім користувачам мережі, кожний закритий ключ, навпаки, зберігається тільки в того абонента, якому він належить. Якщо абонент, скажемо під номером 7, збирається передати інформацію абонентові під номером 9, він шифрує дані ключем шифрування E_9 і відправляє її абонентові 9. Незважаючи на те, що всі користувачі мережі знають ключ E_9 і, можливо, мають доступ до каналу, по якому йде зашифроване послання, вони не можуть прочитати вихідний текст, тому що процедура шифрування необоротна по відкритому ключі. І тільки абонент №9, одержавши послання, робить над ним перетворення за допомогою відомого тільки йому ключа D_9 і відновлює текст послання. Помітьте, що якщо повідомлення потрібно відправити в протилежному напрямку (від абонента 9 до абонента 7), те потрібно буде використовувати вже іншу пару ключів (для шифрування ключ E_7, а для дешифрування – ключ D_7). Як ми бачимо, по-перше, в асиметричних системах кількість існуючих ключів пов'язане з кількістю абонентів лінійно (у системі з N користувачів використовуються 2*N ключів), а не квадратично, як у симетричних системах. По-друге, при порушенні конфіденційності k-ой робочої станції зловмисник довідається тільки ключ D_k : це дозволяє йому читати всі повідомлення, що приходять абонентові k, але не дозволяє видаватися себе за нього при відправленні листів.

Прийом захисту на базі асиметричного шифрування

Розглянемо принципову схему вироблення й перевірки ЕЦП із застосуванням алгоритмів асиметричного шифрування.

Для вироблення ЕЦП підписується документ, що, піддається гешированию (тобто стиску деяким стандартним алгоритмом), а отриманий геш (іноді його називають дайджестом) зашифровується закритим ключем Геширование застосовується для скорочення обсягу шифруемой інформації й підвищення тим самим продуктивності. Геш-Функція, не будучи взаємно однозначним відображенням, підбирається таким чином, щоб було практично неможливо змінити документ, зберігши результат геширования. По гешу неможливо відновити вихідний документ, але це й не потрібно, оскільки перевірка ЕЦП полягає в порівнянні розшифрованої відкритим ключем ЕЦП із гешем документа Збіг з високим ступенем вірогідності гарантує, по-перше, незмінність документа (захист від підробки), і, по-друге, що його підписав власник закритого ключа.

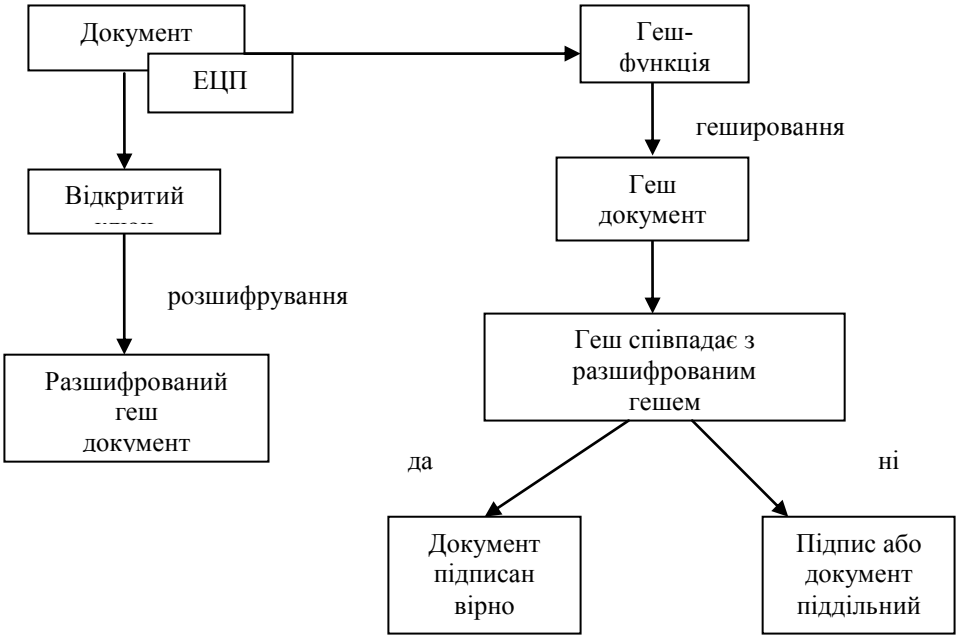

Рис. 1 – Схема перевірки ЄЦП при асиметричному шифруванні

У спеціалізованих криптосистемах, що підтримують тільки технологію ЄЦП, функції властиво шифрування відсутні. Для формування ЕЦП застосовується криптоалгоритм, що одержує на вході геш документа, закритий ключ і що виробляє ЕЦП. Для перевірки ЕЦП застосовується інший криптоалгоритм, що має на вході геш документа що перевіряється ЕЦП і відкритий ключ. Алгоритм перевірки видає позитивний або негативний результат залежно від правильності ЕЦП.

Аутентификация суб'єкта зводиться до доказу того, що він володіє закритим ключем, що відповідає опублікованому відкритому. У криптосистемах, що підтримують технологію ЕЦП, доказ володіння полягає в тім, що суб'єкт підписує своїм закритим ключем присланий йому запит і посилає його назад. Якщо при перевірці виявилося, що запит підписаний правильно, то суб'єкт дійсно має відповідний закритий ключ. Необхідно вжити заходів, щоб

зловмисник, що перехопив підписаний запит, не міг згодом використовувати його, видаючи себе за правомірного власника закритого ключа. Для боротьби із цим досить, щоб запит був неповторюваним.

Асиметричні алгоритми шифрування дозволяють забезпечити конфіденційність при передачі повідомлення від одного суб'єкта іншому. Для цього відправникові досить зашифровувати повідомлення відкритим ключем одержувача. Оскільки розшифрувати повідомлення можна, тільки знаючи відповідний закритий ключ, це гарантує, що прочитати його не зможе ніхто, крім одержувача.

На практиці все повідомлення ніколи не шифрують відкритим ключем. Справа в тому, що продуктивність асиметричного шифрування істотно нижче симетричного, тому звичайно на початку інтерактивного сеансу зв'язку одна зі сторін генерує симетричний секретний ключ (ключ сеансу), шифрує його відкритим ключем іншої сторони й передає тільки цей зашифрований ключ. Інша сторона приймає й розшифровує його (очевидно, при цьому зберігається конфіденційність), а всі подальші повідомлення вже можуть бути зашифровані погодженим ключем сеансу. По закінченні сеансу цей ключ знищується.

Проблема аутентифікації даних й електронний цифровий підпис

При обміні електронними документами по мережі зв'язку істотно знижуються витрати на обробку й зберігання документів, убистряється їхній пошук. Але при цьому виникає проблема аутентифікації автора документа й самого документа, тобто встановлення дійсності автора й відсутності змін в отриманому документі. У звичайній (паперової) інформатиці ці проблеми вирішуються за рахунок того, що інформація в документі й рукописному підписі автора жорстко пов'язані з фізичним носієм (папером). В електронних документах на машинних носіях такого зв'язку немає.

При формуванні ЕЦП відправник насамперед обчислює геш-функцію h(M) тексту, що підписується, M. Обчислене значення геш-функції h(M) являє собою один короткий блок інформації m, що характеризує весь текст M у цілому. Потім число m шифрується секретним ключем відправника. Одержувана при цьому пари чисел являє собою ЕЦП для даного тексту M.

При перевірці ЕЦП одержувач повідомлення знову обчислює геш-функцію m = h(M) прийнятого по каналі тексту M, після чого за допомогою відкритого ключа відправника перевіряє, чи відповідає отриманий підпис обчисленому значенню m геш-функции.

Принциповим моментом у системі ЕЦП є неможливість підробки ЕЦП користувача без знання його секретного ключа підписування.

Як підписиваемого документ може бути використаний будь-який файл. Підписаний файл створюється з непідписаного шляхом додавання в нього однієї або більше електронних підписів.

Кожний підпис містить наступну інформацію:

1. дату підпису;
2. строк закінчення дії ключа даного підпису;
3. інформацію про особу, що підписала файл (Ф.И.О., посада, коротке найменування фірми);
4. ідентифікатор що підписав (ім'я відкритого ключа);
5. властиво цифровий підпис.

Для контролю цілісності електронного документа, доказу його авторства й ідентифікації учасників електронної угоди використовується механізм електронно-цифрового підпису (ЕЦП). Будується вона на ідеології асиметричного шифрування, але використовується як би "навпаки"

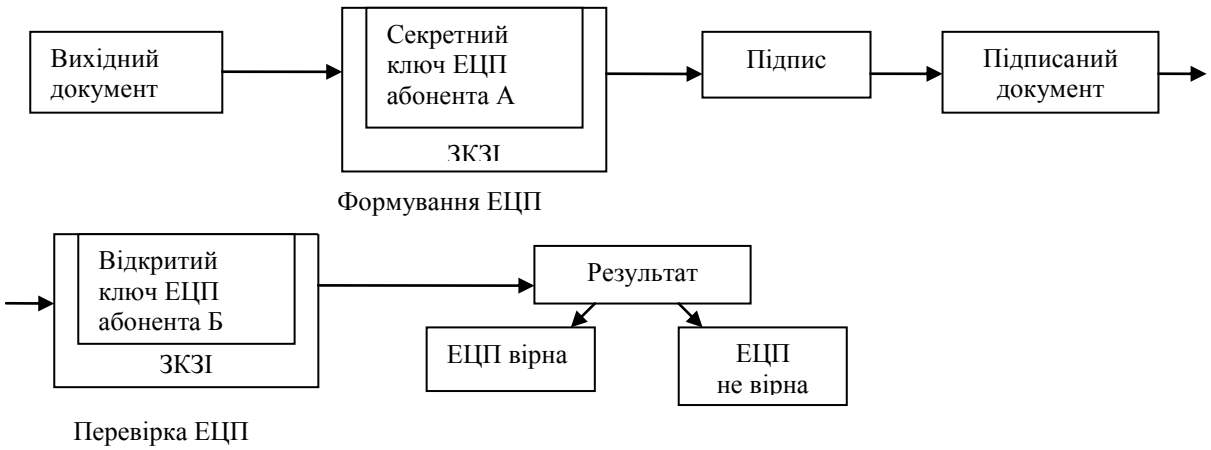

Рис. 2 – Схема формування й перевірки ЄЦП

При виконанні операції обчислення ЕЦП текст документа, що повинен бути підписаний, завантажується в засіб криптографічного захисту інформації (ЗКЗІ). Потім, через те, що шифрування за асиметричною схемою процес повільний, здійснюється обчислення значення так званої геш-функції - послідовності, що відображає, довільної довжини в послідовності фіксованої довжини. Результат обчислення називається геш-кодом, причому по геш-коду

документа відновити його текст не представляється можливим. У стандарті ДЕРЖСТАНДАРТ Р 34.11-94 довжина геш-кода дорівнює 256 биткам. Це означає, що вихідний текст довільної довжини в результаті обробки перетворюється в послідовність із 256 нулів і одиниць. При цьому різні документи не можуть мати однакового геш-кода.

Отриманий геш-код зашифровується з використанням асиметричного алгоритму на секретному ключі абонента А. Тому що довжина геш-кода невелика, операція не займає багато часу. Зашифрований геш-код документа й називається його електронно-цифровим підписом. Обчислена в такий спосіб ЄЦП абонента А передається разом з вихідним документом абонентові Б.

Одержавши текст документа, абонент Б виконує три операції. По-перше, обчислює геш-код повідомлення. По-друге, за допомогою асиметричного алгоритму й відкритого ключа абонента А розшифровує отриману разом з документом його ЕЦП. По-третє, порівнює результат расшифрования з обчисленим геш-кодом. У випадку збігу робиться висновок про те, що підпис вірний: автором документа дійсно є абонент А и після того як документ був підписаний, ніяких змін у його текст не вносилося.

Дійсно, якщо в процесі передачі в текст документа була внесена зміна (навмисне або випадкове), те обчислений абонентом Б геш-код буде відрізнятися від того, котрий він одержить після расшифрования ЕЦП. Результат порівняння буде негативним і в тому випадку, якщо для формування ЕЦП був використаний ключ, відмінний від секретного ключа абонента А.

При веденні ділової переписки, при висновку контрактів підпис відповідальної особи є неодмінним атрибутом документа, що переслідує кілька мет:

1. Гарантування істинності листа шляхом звірення підпису з наявним зразком;
2. Гарантування авторства документа (з юридичної точки зору)
3. Виконання даних вимог ґрунтується на наступних властивостях підпису:
4. підпис автентичний, тобто з її допомогою одержувачеві документа можна довести, що вона належить що підписує;
5. підпис неподделиваема; тобто є доказом, що тільки та людина, чий автограф стоїть на документі, міг підписати даний документ, і ніхто інший.
6. Підпис нестерпний, тобто є частиною документа й тому перенести її на інший документ неможливо.
7. Документ із підписом є незмінним.
8. Підпис незаперечний.
9. Будь-яка особа, що володіє зразком підпису може впевниться, що документ підписаний власником підпису.

Висновок

Розвиток сучасних засобів безпаперового документообігу, засобів електронних платежів немислимо без розвитку засобів доказу дійсності й цілісності документа. Таким засобом є електронно-цифровий підпис (ЕЦП), що зберегла основні властивості звичайного підпису.

Існує кілька методів побудови ЕЦП, а саме:

шифрування електронного документа (ЕД) на основі симетричних алгоритмів. Дана схема передбачає наявність у системі третьої особи - арбітра, що користується довірою обох сторін. Авторизацією документа в даній схемі є сам факт зашифрування ЕД секретним ключем і передача його арбітрові.

Використання ассиметричних алгоритмів шифрування. Фактом підписання документа є зашифрування його на секретному ключі відправника.

Розвитком попередньої ідеї стала найпоширеніша схема ЕЦП - зашифрування остаточного результату обробки ЕД геш-функцією за допомогою ассиметричного алгоритму.

Крім перерахованих, існують і інші методи побудови схем ЕЦП

- груповий підпис, що не заперечується підпис, довірена підпис і ін. Поява цих різновидів обумовлено розмаїтістю завдань, розв'язуваних за допомогою електронних технологій передачі й обробки електронних документів.

Список використаних джерел

[1] Смарт Н. Криптография.-М: Техносфера, 2005. -528с.
[2] Молдовян Н.А., Молдован А.А. Введение в криптосистемы с открытым ключом. - СПб.: БХВ - Петербург, 2005. - 288 с. : ил.
[3] Молдовян Н.А. Практикум по криптосистемам с открытым ключом. - СПб.: БХВ -Петербург, 2007. - 304 с: ил.Математические и компьютерные основы криптологии: Учеб пособие / Ю.С. Харин В.И. Берник, Г.В. Матвеев, С.В. Агиевич. -Мн.: Новое знание, 2003. - 382 с.
[4] Фергюсон Н., Шнайер Б. Практическая криптография: Пер. с англ. - М.: Изд. Дом «Вильямс», 2005. - 424е.
[5] ОсипянВ.О., ОсипянК.В. Криптография в задачах и упражнениях.-М.: Гелиос АРВ, 2004.-144с.
[6] Криптографические методи защити информации. Совершенные шифры: Учеб. пособие/ А.Ю. Зубов. -М.: Гелиос АРВ, 2005. - 192с.
[7] Мао, Венбо. Современная криптография: теория и практика: Пер. с англ. - М: Изд. Дом «Вильямс», 2005. -768с.
[8] Введение в криптографию / Под ред. В.В. Ященко. -М.: 1998.
[9] Зашита информации в персональних ЗВМ / А.В.Спесивцев, В.А. Вегнер, А.Ю.Крутяков, В.В.Сгрегин, ВЛСидоров. -М., 1993.

[10] Коблиц Н. Курс теории чисел и криптографии.-М., 2001.
[11] Нечаев В.И. Элементы криптографии. Основы теории защиты информации. - М., 1999.
[12] Лекции по дискретной математике / Ю.В.Капитонова, С.Л. Кривой, А.А.Летичевский, Г.М. Луцкий / СПб.: БХВ ~ Петербург, 2004. - 624с.
[13] Романец Ю.В., Тимофеєв П.А., Шаньгин В.Ф. Зашита информации в компьютерьгх системах и сетях. - М.: Радио и связь. - 1999, 328 с.
[14] Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей. - Изд - во: Форум, 2О07.-416с.
[15] Саломаа А. Криптография с открытым ключом: Пер с англ.-М.: Мир, 1996. - 304 с.
[16] Шеннон К.З. Теория связи в секретных системах. В кн. К.Э. Шеннона. "Работы по теории информации и кибернетике". - М.: ИЛД963.- С. 243-332.
[17] Жельников В. Криптография от папируса до компьютера. -М.:АВГ,1997.-336 с.
[18] Виноградов И.М. Основы теории чисел -М.: Наука, 1981.
[19] Питерсон У., Уэлдон Э. Коды, исправляющие ошибки. Пер. с англ.-М.: Мир,1976. - 594с.
[20] Диффи У.} Хеллман М.Э. Защишенность и имитостойкость. Введение в криптографию //ТИИЗР.-1979. - Т.67, №3. - С. 71-109.
[21] Месси Дж. Л. Введение в современную криптологию // ТИИЗР.-1988.-Т.76, №5. - С.24 -47.
[22] Смид М.Э., Бранстед Д.К. Стандарт шифрования данных. Прошлое и будущее // ТИИЗР. -1988.-Т.76.- №5. -С.43-53.
[23] В.Столлингс.Криптография и защита сетей. Принципи и практика. Изд-во Диалектика -2001. ~ 672с.
[24] Правильный выбор криптографических средств: Обзор современной криптографической техники (по материалам зарубежной печати) // Защита информации. - 1994.-№1.-С.42-47.
[25] ЧмораАЛ.Критггосистема с депонированием ключа//Соп пес 1997. - №3 - С.34-39.
[26] ГОСТ Р 34.10 - 94. Информационная технопогия. Криптографическая защита информации Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма.

References

[1] Smart N. Kryptohrafyya.-M: Tekhnosfera, 2005. -528p.
[2] Moldovyan N.A., Moldovan A.A. Vvedenye v kryptosystemy s otkrytym klyuchom. - SPb.: BKhV - Peterburh, 2005. - 288 p. : yl.
[3] Moldovyan N.A. Praktykum po kryptosystemam s otkrytym klyuchom. - SPb.: BKhV -Peterburh, 2007. - 304 s: yl.Matematycheskye y komp'yuternye osnovy kryptolohyy: Ucheb posobye / Yu.S. Kharyn V.Y. Bernyk, H.V. Matveev, S.V. Ahyevych. -Mn.: Novoe znanye, 2003. - 382 p.
[4] Ferhyuson N., Shnayer B. Praktycheskaya kryptohrafyya: Per. s anhl. - M.: Yzd. Dom «Vylyams», 2005. – 424p.
[5] OsypyanV.O., OsypyanK.V. Kryptohrafyya v zadachakh y uprazhnenyyakh.-M.: Helyos ARV, 2004.-144s.
[6] Kryptohrafycheskye metody zashchyty ynformatsyy. Sovershennye shyfry: Ucheb. posobye/ A.Yu. Zubov. -M.: Helyos ARV, 2005. – 192 p.
[7] Mao, Venbo. Sovremennaya kryptohrafyya: teoryya y praktyka: Per. s anhl. - M: Yzd. Dom «Vylyams», 2005. -768p.
[8] Vvedenye v kryptohrafyyu / Pod red. V.V. Yashchenko. -M.: 1998.
[9] Zashyta ynformatsyy v personalnykh ZVM / A.V.Spesyvtsev, V.A. Vehner, A.Yu.Krutyakov, V.V.Shrehyn, VLSydorov. -M., 1993.
[10] Koblyts N. Kurs teoryy chysel y kryptohrafyy.-M., 2001.
[11] Nechaev V.Y. Elementy kryptohrafyy. Osnovy teoryy zashchyty ynformatsyy. - M., 1999.
[12] Lektsyy po dyskretnoy matematyke / Yu.V.Kapytonova, S.L. Kryvoy, A.A.Letychevskyy, H.M. Lutskyy / SPb.: BKhV ~ Peterburh, 2004. – 624p.
[13] Romanets Yu.V., Tymofeyev P.A., Shanhyn V.F. Zashyta ynformatsyy v kompyuternykh systemakh y setyakh. - M.: Radyo y svyaz. - 1999, 328 p.
[14] Shanhyn V.F. Ynformatsyonnaya bezopasnost kompyuternykh system y setey. - Yzd - vo: Forum, 2O07.-416 p.
[15] Salomaa A. Kryptohrafyya s otkrytym klyuchom: Per s anhl.-M.: Myr, 1996. - 304 p.
[16] Shennon K.Z. Teoryya svyazy v sekretnykh systemakh. V kn. K.E. Shennona. "Raboty po teoryy ynformatsyy y kybernetyke". - M.: YLD963.- P. 243-332.
[17] Zhelnykov V. Kryptohrafyya ot papyrusa do kompyutera. -M.:AVH,1997.-336 p.
[18] Vynohradov Y.M. Osnovy teoryy chysel -M.: Nauka, 1981.
[19] Pyterson U., Ueldon E. Kody, yspravlyayushchye oshybky. Per. s anhl.-M.: Myr,1976. – 594 p.
[20] Dyffy U. Khellman M.E. Zashchyshennost y ymytostoykost. Vvedenye v kryptohrafyyu //TYYZR.-1979. - T.67, №3. - P. 71-109.
[21] Messy Dzh. L. Vvedenye v sovremennuyu kryptolohyyu // TYYZR.-1988.-T.76, №5. - P.24 -47.
[22] Smyd M.E., Bransted D.K. Standart shyfrovanyya dannykh. Proshloe y budushchee // TYYZR. -1988.-T.76.- №5. -P.43-53.
[23] V. Stollynhs. Kryptohrafyya y zashchyta setey. Pryntsypy y praktyka. Yzd-vo Dyalektyka -2001. - 672 p.
[24] Pravylnyy vybor kryptohrafycheskykh sredstv: Obzor sovremennoy

kryptohrafycheskoy tekhnyky (po materyalam zarubezhnoy pechaty) // Zashchyta ynformatsyy. - 1994.-№1.-P.42-47.
[25] ChmoraA L. Krythhosystema s deponyrovanyem klyucha//Sop pes 1997. - №3 - P.34-39.
[26] HOST R 34.10 - 94. Ynformatsyonnaya tekhnopohyya. Kryptohrafycheskaya zashchyta ynformatsyy Protsedury vyrabotky y proverky èlektronnoy tsyfrovoy podpysy na baze asymmetrychnoho kryptohrafycheskoho alhorytma.

УДК 66.012:66.048.3

МАТЕМАТИЧНЕ МОДЕЛЮВАННЯ ДИНАМІЧНИХ РЕЖИМІВ ПРОЦЕСУ РЕКТИФІКАЦІЇ ПРИ ЗАСТОСУВАННІ РУХЛИВИХ КЕРУЮЧИХ ВПЛИВІВ

Шейкус А. Р.

Український державний хіміко-технологічний університет, Дніпро, Україна
ORCID: https://orcid.org/0000-0002-5575-098X
E-mail: a.sheykus@gmail.com

DOI:

Анотація. *Підвищення якості керування об'єктами з розподіленими параметрами, до яких відноситься процес ректифікації, можливо досягти використанням рухливих впливів. Відомо, що переміщення за висотою колони точки подання живлення або перерозподіл даного потоку між двома контактними пристроями апарату дозволяє забезпечити недосяжні традиційним керуванням техніко-економічні показники стаціонарних режимів. При цьому перехідні процеси в колоні при використанні рухливих впливів залишалися недослідженими.*

У статті розроблено математичну модель динаміки процесу ректифікації, що враховує рухливі керуючі впливи, а також досліджено особливості динамічних режимів роботи колони при їх використанні. В моделі передбачено можливість реалізації різних за формами і інтенсивностями збурень і керуючих впливів за декількома каналами одночасно або у визначені моменти часу. Модель дозволяє проводити розрахунки процесів багатокомпонентної і складної ректифікації, може використовуватися при моделюванні пускових режимів.

Процес ректифікації внаслідок використання рухливих впливів виходить зі стану динамічної рівноваги. Встановлено, що новий стаціонарний режим досягається регулюванням тиску наверху колони, рівнів в ємностях для збору кубового залишку і дистиляту. Запропоновано використання ПІД-регуляторів з впливами на витрати холодоагенту в конденсатор і продуктів поділу. Динамічна модель процесу доповнена описом даних контурів автоматичного регулювання.

З використанням розробленої моделі проведено обчислювальні експерименти на прикладі колони для поділу суміші метанол-вода. Доведено, що перехідні процеси при використанні рухливих керуючих впливів на процес ректифікації характеризуються допустимими показниками якості.

Abstract. *Improving the control quality of objects with distributed parameters, including the rectification process, could be achieved by using mobile actions. It is known that moving along the column height of the feed supply point or redistributing a given flow between the apparatus’ two contact devices allows getting the technical and economic indicators of stationary modes unattainable by using traditional control. Also, the transient responses in the column when using movable influences remained unstudied.*

The article developed a mathematical model of the distillation process dynamics, considering mobile control actions, as well as there have been studied the dynamic modes’ features of column operation when used them. The model allows implementing disturbances and control actions of various kinds and intensities via several channels simultaneously or at certain points of time. The model allows computing the processes of multicomponent and complex distillation, and can be used to compute the starting modes.