УДК 004.056.55

В.Ю. ШАДХІН, Е.В. ФАУРЕ
Черкаський державний технологічний університет
О.В. КОСТОМАРОВ
Київський національний університет технологій та дизайну

КРИПТОГРАФІЧНІ ЗАСОБИ ЗАХИСТУ ІНФОРМАЦІЇ В АВТОМАТИЗОВАНИХ СИСТЕМАХ ДИСТАНЦІЙНОГО НАВЧАННЯ

В статті розроблено алгоритм захисту дистанційної навчальної системи шляхом шифрування даних, які організовують захист інформації та обмін нею з використанням ідеології відкритого ключа без використання додаткових апаратних засобів, який при подальший практичній реалізації надасть змогу зменшити вартість технічного забезпечення засобів дистанційної освіти, а отже і зменшити вартість навчання.

In the article developed an algorithm for protection of remote learning system by encrypting the data, which organize the protection and exchange of information with the ideology of the public key without any additional hardware, which in the further implementation will reduce the cost of technical support of distance education, and thus reduce the cost of education.

Ключові слова: дистанційна освіта, захист інформації в системах дистанційної освіти.

Постановка задачі

Безперервна освіта є загальним показником тенденції підвищення ролі і значення постійного навчання людини відповідно до швидкого оновлення знань. В той же час сьогодні з'являється можливість використання широких освітніх середовищ і нових навчальних технологій.

Інформаційні технології вже давно проникли в галузь освіти. Дистанційне навчання з використанням інтернет-технологій є сучасною формою одержання освіти, поряд з стаціонарною та заочною. Всесвітня мережа Інтернет надає великі можливості для установ освіти. У дистанційному освітньому процесі використовуються кращі традиційні й інноваційні методи, засоби і форми навчання, засновані на комп'ютерних і телекомунікаційних технологіях.

В даний час більшість фахівців у галузі освіти покладають надії на сучасні персональні комп'ютери, розраховуючи з їх допомогою істотно підвищити якість навчання в масових масштабах, особливо в організації самостійної роботи та зовнішньому контролі. Але при здійсненні цього завдання виникає безліч проблем. Однією з яких є забезпечення інформаційної безпеки в системах дистанційного навчання.

Завдання забезпечення інформаційної безпеки в системах дистанційного навчання.

Завдання забезпечення інформаційної безпеки в системах дистанційного навчання, близькі до аналогічних завдань в інших системах обробки інформації, для розв`язання яких на даний момент вже існує законодавча і нормативна база, а також організаційні та технічні рішення. Захист інформації в системі дистанційного навчання має свою специфіку [2]. В якості головних особливостей можна вказати:

- територіально розподілена структура;
- різнорідність використовуваних програмних і технічних рішень;
- необхідність захисту інформації та інтелектуальної власності, що належить декільком власникам одночасно.

Під інформаційною безпекою дистанційного навчання розуміється стан захищеності його інтересів від існуючих і ймовірних зовнішніх і внутрішніх загроз інформаційних ресурсів [1].

Інформаційними ресурсами є:

- технічні засоби дистанційного навчання (комп'ютерна техніка та засоби зв'язку);
- електронні носії всіх типів і видів;
- інформація у вигляді файлів і баз даних на електронних носіях;
- архіви та електронні бібліотеки.

Надійність інформації в системі дистанційного навчання – це інтегральний показник, що характеризує якість інформації з точки зору:

- фізичної цілісності, тобто наявності або відсутності спотворень або знищення елементів цієї інформації;
- довіри до інформації, тобто наявності або відсутності в ній підміни (несанкціонованої модифікації інформації) її елементів при збереженні цілісності;
- безпеки інформації, тобто наявності або відсутності несанкціонованого отримання інформації особами чи процесами, які не мають на це відповідних повноважень;
- впевненості в тому, що передані або продані власником програми або елементи баз (масивів) даних не будуть розмножуватися (копіюватися, тиражуватися) і використовуватися без його санкції.

Завданнями забезпечення інформаційної безпеки і відповідно функціями системи забезпечення інформаційної безпеки є:

- припинення та виявлення спроб знищення або підміни (фальсифікації) інформації;
- припинення та виявлення спроб несанкціонованої модифікації інформації;
- припинення та виявлення спроб несанкціонованого отримання інформації;

- припинення та виявлення спроб несанкціонованого розповсюдження або розмноження інформації;
- ліквідація наслідків успішної реалізації перерахованих загроз;
- виявлення та нейтралізація потенційно можливих дестабілізуючих факторів і каналів витоку інформації;
- виявлення та нейтралізація причин проявів дестабілізуючих факторів і виникнення каналів витоку інформації;
- визначення осіб, винних у прояві дестабілізуючих факторів і виникненні каналів витоку інформації, і притягнення їх до певного виду відповідальності.

Мета заходів щодо забезпечення інформаційної безпеки – скоротити можливий економічний і моральний збиток, пов'язаний з пошкодженням чи неправомірним використанням інформаційних ресурсів.

Забезпечення інформаційної безпеки являє собою складний комплекс технічних, юридичних і організаційних проблем.

Основою для системного вирішення завдань забезпечення інформаційної безпеки є аналіз можливих ризиків, політика інформаційної безпеки та план забезпечення інформаційної безпеки.

Аналіз ризиків – перший і необхідний етап у розв'язанні задачі захисту інформації, він проводиться з метою виявлення переліку потенційно можливих загроз безпеки дистанційного навчання, які можуть виникнути в результаті реалізації таких ризиків.

На основі результатів аналізу ризиків розробляється політика безпеки – документ, що містить принципи діяльності дистанційного навчання, щодо проблем інформаційної безпеки. Політика безпеки містить перелік загроз, які приймаються до уваги, класифікацію інформаційних ресурсів, які захищаються, визначає бажаний рівень захищеності, описує організаційні рішення, необхідні для розв`язання завдань інформаційної безпеки. На основі затвердженої політики безпеки розробляється план забезпечення інформаційної безпеки, що містить конкретні організаційні та технічні рішення і плани робіт по їх впровадженню і реалізації [3].

Для розробки політики інформаційної безпеки в системах дистанційного навчання необхідно проаналізувати їх структуру.

Загальна структура системи дистанційного навчання.

Загальну структуру системи дистанційного навчання можна представити в наступному вигляді. Є сховище даних (сховище), яке надає необхідні матеріали (лекції, фільми, аудіозаписи) і сервіси (програмне забезпечення, консультації і т.д.) віддаленим студентам за допомогою публічних комп'ютерних мультимедійних мереж (найчастіше Інтернет). Студент може представляти на розгляд викладачу результати своєї роботи, використовуючи комп'ютерну мережу.

Студент проходить реєстрацію, яка визначає для віддалених студентів доступ до матеріалів, розміщених в репозиторії. Далі студент починає навчання, яке представляє собою отримання навчального матеріалу, його засвоєння та проходження тестування знань. Вважається, що при деяких умовах студенти можуть побажати призупинити навчання на тривалий період, а далі знову відновити його. За деяких обставин (наприклад, якщо протягом певного періоду часу студент не зміг завершити етап хоча б з мінімально допустимої оцінкою) робота студента може бути припинена [4].

Проаналізувавши структуру системи дистанційного навчання, можна сказати, що необхідно приділяти увагу безпеці в наступних областях:

- віддалена автентифікація студента;
- контроль доступу;
- виявлення вторгнення;
- захист мережевих комунікацій;
- гарантованість доставки;
- захист сховища даних.

Автентифікація студента – перевірка приналежності суб'єкту доступу пред'явленого ним ідентифікатора; підтвердження автентичності особи. Вона може базуватися на традиційних парольних механізмах, які можуть бути легко реалізовані програмними методами. Одне з можливих удосконалень – використовувати автентифікацію на основі місця розташування за допомогою постійної IP-адреси або послуги зворотного дзвінку, коли студенти підключаються до навчальної системи. Але ця стратегія має недоліки, наприклад, віддалений студент змушений завжди підключатися до освітньої системи з одного і того ж місця, що порушує принцип мобільності дистанційної освіти.

Більш складні схеми автентифікації користувача використовують технології смарт-карт, для побудови сильних систем авторизації з простим призначеним для користувача інтерфейсом. Їх основна перевага полягає у безпечному зберіганні та обробці секретної інформації – ключова конфеденційна інформація зберігається тільки на смарт-карті і ніде більше. Основний недолік смарт-карт перед парольною системою – це збільшення вартості.

Бажано, щоб механізми автентифікації були однакові для всіх модулів дистанційної освітньої системи, з метою простоти використання системи для студента.

Після успішного підключення до системи, доступ до інформації повинен бути проконтрольований за допомогою електронних сертифікатів, які підтверджують проходження студентом певного етапу

навчання і можливість переходу до наступного. Ці засоби повинні використовуватися як додаток до вже існуючих засобів контролю доступу, що надаються операційною системою.

Система виявлення вторгнення може представляти із себе систему моніторингу в режимі реального часу, яка порівнює поведінку авторизованого користувача з минулими записами його поведінки для визначення автентичності користувача. Такі записи можуть складатися з ряду факторів, серед яких час підключення до системи, використання різних сервісів і дані, до яких запитаний доступ. Цей підхід повністю реалізований програмними засобами і не вимагає додаткових витрат. Недоліками його є можливість відмови від авторизації легального користувача, а також невдоволення користувачів тим, що їх дії докладно записуються.

Захист мережевих комунікацій може бути досягнутий за допомогою шифрування даних. Можна вибрати гібридну систему, де симетрична криптографія використовується для досягнення конфіденційності (загальні секретні ключі для системи і студента), а асиметрична криптографія використовується для розподілу сесійних ключів і для гарантованості доставки (ґрунтуючись на електронно-цифровому підписі).

Вимоги для гарантованості доставки виникають як з боку студента, так і з боку системи і служать для запобігання відмов від:

- відправки повідомлення (підтвердження того, що студент – автор роботи);
- прийому повідомлення (підтвердження того, що робота була прийнята системою);
- змісту повідомлення (підтвердження того, що повідомлення не було модифіковано в процесі доставки).

Гарантованість відправки та прийому повідомлення може бути досягнута використанням цифрового підпису, коли комунікації "підписані" стороною, що відправляє повідомлення, за допомогою секретного ключа. Підтвердження незмінності змісту може бути досягнуто через використання коду автентифікації повідомлення (message authentication code – MAC), які є результатом цифрової обробки повідомлення. Операція обробки повідомлення побудована таким чином, щоб будь-які зміни змісту повідомлення викликало б зміну в MAC, що дозволяє ефективно контролювати цілісність повідомлення.

Проблеми безвідмовності роботи вирішуються загальноприйнятими методами, використовуваними в усіх комп'ютерних системах: питання резервного копіювання і відновлення, фізичний захист для установи навчальної системи та інші. Доступність і надійність системи вкрай важлива. Студент повинен мати можливість доступу до системи в будь-який час, тому високий рівень безвідмовності для системи дистанційного навчання вкрай необхідний [5].

Постановка завдання

Метою дослідження є аналіз засобів захисту інформації АСДН без використання допоміжних апаратних засобів. Для того, щоб відмовитися від використання дорогих апаратних засобів, необхідно розробити програмне забезпечення захисту дистанційної навчальної системи шляхом шифрування даних, яка б ґрунтувалося на використанні множини унікальних поліморфних алгоритмів, та організувати захист інформації та обмін нею з використанням ідеології відкритого ключа, яка також ґрунтується на поліморфних алгоритмах.

Результати та їх обговорення

Розглянемо поліморфний алгоритм шифрування даних, побудований на основі асиметричної криптосистеми, а саме криптосистему Ель-Гамаля, з використанням еліптичних кривих.

Асиметричні криптосистеми – ефективні системи криптографічного захисту даних, які також називають криптосистемами з відкритим ключем. В таких системах для зашифровування даних використовується один ключ, а для розшифровування – інший ключ. Перший ключ є відкритим і може бути опублікованим для використання усіма користувачами системи, які шифрують дані. Розшифровування даних за допомогою відкритого ключа неможливе. Для розшифровування даних отримувач зашифрованої інформації використовує інший ключ, який є секретним. Зрозуміло, що ключ розшифровування не може бути визначеним з ключа шифрувування.

Асиметрична криптографія заснована на складності вирішення деяких математичних задач. Ранні криптосистеми з відкритим ключем, такі як алгоритм RSA, безпечні завдяки тому, що складно розкласти складене число на прості множники. Використання алгоритмів на еліптичних кривих полягає в тому, що не існує субекспоненціальних алгоритмів для розв`язання задачі дискретного логарифмування в групах їх точок. При цьому порядок групи точок еліптичної кривої визначає складність завдання. Вважається, що для досягнення такого ж рівня безпеки як і в RSA потрібні групи менших порядків, що зменшує витрати на зберігання та передачу інформації [4].

Еліптична криптографія – розділ криптографії, який вивчає асиметричні криптосистеми, засновані на еліптичних кривих над кінцевими полями. Як вже зазначалося раніше, основна перевага еліптичної криптографії полягає в тому, що на сьогоднішній день не відомо субекспоненціальних алгоритмів для розв`язання задачі дискретного логарифмування в групах точок еліптичних кривих.

Схема Ель-Гамаля (Elgamal) – криптосистема з відкритим ключем, заснована на складності обчислення дискретних логарифмів в кінцевому полі. Криптосистема включає в себе алгоритм шифрування і алгоритм цифрового підпису. Схема Ель-Гамаля лежить в основі стандартів електронного цифрового підпису.

Опишемо систему побудовану на основі криптосистеми Ель-Гамаля, з використанням еліптичних

кривих.

Для шифрування і дешифрування текстів, за допомогою еліптичних кривих використовуються декілька методів. Один з них полягає в тому, щоб моделювати криптосистему Ель-Гамаля, використовуючи еліптичну криву в $GF(p)$ або $GF(2n)$, як це показано на рисунку 1.

Генерація загальнодоступних і приватних ключів:

1) Студент обирає $E_p(a, b)$ з еліптичної кривої в $GF(p)$ або $GF(2n)$.

2) Студент обирає точку на кривій, $e_1(x_1, y_1)$.

3) Студент обирає ціле число d.

4) Студент обчислює $e_2(x_2, y_2) = d * e_1(x_1, y_1)$. Зверніть увагу: множення означає, що багаторазове складання визначається як раніше.

5) Студент оголошує $E_p(a, b)$, $e_1(x_1, y_1)$ і e2 (x2, y2), як свій відкритий ключ доступу; він зберігає d як секретний ключ.

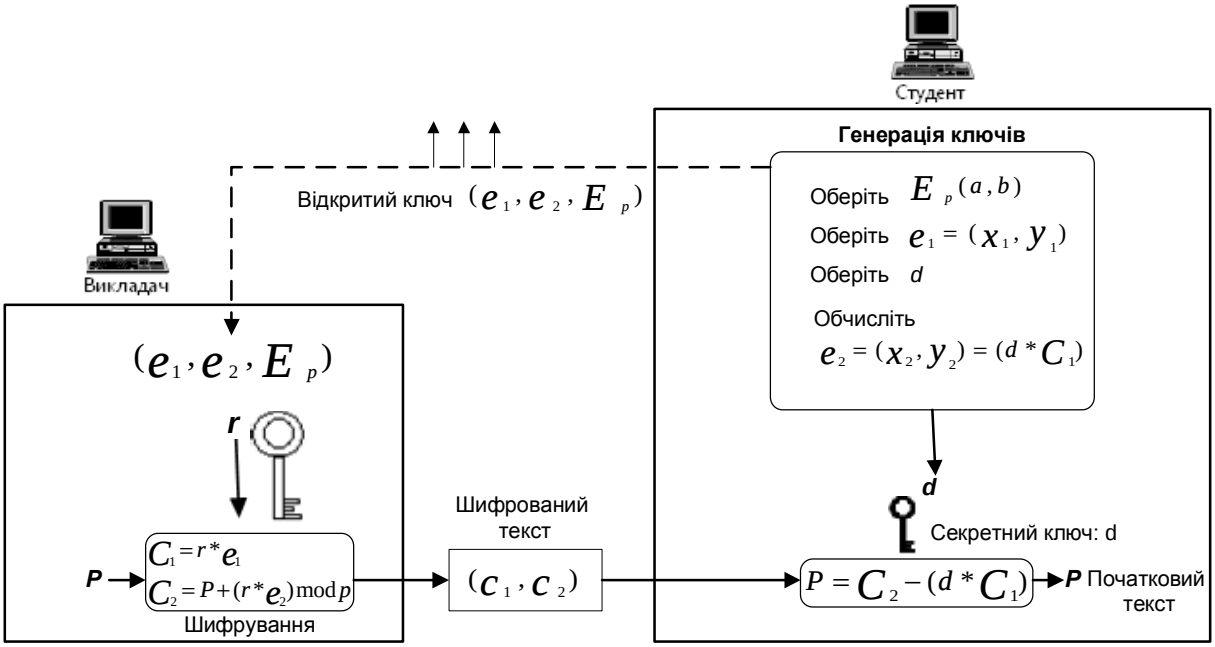

Рис. 1. Криптосистема Ель-Гамаля, з використанням еліптичної функції

Шифрування:

Викладач обирає P, точку на кривій, як її вихідний текст, P. Потім він обчислює пару точок, направляє як зашифрований текст:

$C_1 = r * e_1$; $C_2 = P + r * e_2$ Точка на еліптичній кривій може бути довільним вихідним текстом. Для цього, викладач повинен використовувати алгоритм, щоб знайти безпосередню відповідність між символами (або блоками тексту) і точками на кривій.

Дешифрування:

Студент, після отримання C_1 і C_2, обчислює P, вихідний текст, використовуючи наступну формулу:

$P = C_2 - (d * C_1)$ Знак "мінус" означає додавання з інверсією.

Можна довести, що P, обчислений студентом, – той же, що переданий викладачем, як це показано нижче:

$$P + r * e_2 - (d * r * e_1) =$$
$$= P + (r * d * e_1) - (r * d * e_1) = P + 0 = P,$$

де P, C_1, C_2 та e_2 – це точки на кривій. Зверніть увагу, що результат складання двох зворотних точок на кривій – нульова точка.

Наведемо тривіальний приклад шифрування з використанням еліптичної кривої в $GF(p)$.

Студент вибирає E67 (2, 3) як еліптичну криву в $GF(p)$.

Студент обирає e_1 = (2, 22) і d = 4.

Студент обчислює e_2 = (13, 45), де $e_2 = d * e_1$.

Студент публічно оголошує кортеж (E, e_1, e_2).

Викладач хоче передати вихідний текст P = (24, 26) студенту. Він обирає r = 2.

Викладач знаходить точку C_1 = (35, 1), де $C_1 = r * e_1$.

Викладач знаходить точку C_2= (21, 44), де $C_2 = P * e_1$.

Студент отримує C_1, і C_2. Він використовує $2 * C_1$, (35, 1) і отримує (23, 25).

Студент інвертує точку (23, 25) і отримує точку (23, 42).

Студент складає (23, 42) з C_2 = (21, 44) і отримує початковий вихідний текст P = (24, 26).

Наведемо коротке порівняння алгоритму Ель-Гамаля з його варіантом, що використовує еліптичну криву.

1) Алгоритм Ель-Гамаля використовує мультиплікативну групу, алгоритм криптосистеми Ель-Гамаля, з використанням еліптичних кривих – еліптичну групу.

2) Ці два члени в алгоритмі Ель-Гамаля – числа мультиплікативної групи, при застосуванні алгоритму Ель-Гамаля, з використанням еліптичних кривих, це точки на еліптичній кривій.

3) Секретний ключ в кожному алгоритмі – ціле число.

4) Секретні числа, обрані викладачем в кожному алгоритмі – цілі числа.

5) Піднесення до степеня в алгоритмі Ель-Гамаля замінено множенням точки на константу.

6) Множення в алгоритмі Ель-Гамаля замінено складанням точок.

7) Інверсія в алгоритмі Ель-Гамаля – мультиплікативна інверсія в мультиплікативній групі, в алгоритмі Ель-Гамаля, з використанням еліптичних кривих, інверсія-замінюється адитивною інверсією точки на кривій.

8) Обчислення зазвичай легше в еліптичної кривої, тому що множення простіше, ніж зведення в степінь, складання простіше, ніж множення, і знаходження інверсії набагато простіше в групі еліптичної кривої, ніж у мультиплікативної групи.

Безпека методу з використанням еліптичної кривої

Щоб розшифрувати повідомлення, зловмисник повинен знайти значення r або d.

1) Якщо зловмисник знає значення r, він може використати $P = C_2 - (r * e_2)$, щоб знайти точку P, що відноситься до початкового тексту. Але для того, щоб знайти r, зловмисник повинен вирішити рівняння $C_1 = r * e_1$. Це означає – знайти дві точки на кривій, C_1 і e_1. Зловмисник повинен знайти множник, який створює C_1 починаючи з e_1. Ця проблема відома як проблема логарифма еліптичної кривої, єдиний відомий метод вирішення цієї проблеми – ρO (ρ) – алгоритм Поларда, розв'язок якого неможливий, якщо задано велике r і p в $GF(p)$ або велике n в $GF(2n)$.

2) Якщо зловмисник знає значення d, він може використати $P = C_2 - (d * C_1)$, щоб знайти точку P, що відноситься до початкового тексту. Оскільки $e_2 = d * e_1$, це той же тип проблеми, що і в попередньому пункті. Зловмисник знає значення e_1 і e_2 – він повинен знайти d.

Отже можна зробити висновок, що безпека криптосистеми з еліптичною кривою залежить від трудності вирішення проблеми логарифма еліптичної кривої.

Висновки

З проведеного дослідження можна зробити висновок, що реалізація захисту інформації систем дистанційного навчання породжує безліч вимог, які повинні бути проаналізовані та задоволені. Надання необхідного рівня безпеки та конфіденційності є необхідною умовою для нормального функціонування і подальшого розвитку систем дистанційної освіти.

Також під час дослідження було розроблено алгоритм захисту дистанційної навчальної системи шляхом шифрування даних, які організовують захист інформації та обмін нею з використанням ідеології відкритого ключа без використання додаткових апаратних засобів, який при подальший практичній реалізації надасть змогу зменшити вартість технічного забезпечення засобів дистанційної освіти, а отже і зменшити вартість навчання.

Література

1. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей : [уч. пособ.] / Шаньгин В.Ф. – М. : Форум, 2008. – 416 с.

2. Ложников П.С. Распознавание пользователей в системах дистанционного образования: обзор / П.С. Ложников // Educational Technology & Society. – 2001. – № 4.

3. Ерижоков А.А. Использование VMWare 2.0 [Електронний ресурс] / А.А. Ерижоков // Публікація у мережі інтернет на сервері. – Режим доступу : http://www.citforum.ru/operating_systems/vmware/index.shtml

4. Касперский Е.В. Компьютерные вирусы: что это такое и как с ними бороться / Касперский Е.В. – М. : СК Пресс, 1998. – 288 с.

5. Баричев С.Г. Основы современной криптографии / Баричев С.Г. – М. : Горячая линия – Телеком, 2001. – 120 с.

Надійшла 8.12.2011 р.
Рецензент: д.т.н. Рудницький В.М.