структурної надійності на основі оцінок Езарі-Прошана. Використання цього методу дає змогу істотно скоротити обсяг обчислень, необхідних для одержання оцінки із заданою точністю.

Практичне застосування того або іншого методу визначається постановкою завдання, наявним парком обчислювальної техніки, ступенем точності вихідних ймовірностей $w(t_i)$ безвідмовного обслуговування заявок на елементах і розмірністю оцінюваної телекомунікаційної системи.

*Список використаної література:* ***1.*** *Надійність техніки. Терміни та визначення: ДСТУ 2860-94 – [Чинний від1996–01–01]. – К.:Держспоживстандарт України, 1996. – 76 с. – (Національний стандарт України).* ***2.*** *Щербина Л. П. Основы теории сетей военной связи. – Л.: ВАС, 1984. – 170 с.* ***3.*** *Вермишев Ю. Х. Методы автоматического поиска решений при проектировании сложных технических систем. – М.: Радио и связь, 1982. –152 с.* ***4.*** *Кутузов О. И. Татарникова Т. М. Моделирование телекоммуникационных сетей. – С.-П.: СПГУТ, 2005, – 80 с.* ***5.*** *Мизин И. А., Богатырев В. А., Кулешов А. П. Сети коммутации пакетов / Под ред. В. С. Семенихина. – М.: Радио и связь, 1986. – 408 с.* ***6.*** *Гадасин В. А. Методы расчета структурной надежности сетей связи. – М.: 1986.* ***7.*** *Волик В. Г., Рябинин И. А. Эффективность, надежность и живучесть управляющих систем. / Автоматика и телемеханика, 1984, № 12.* ***8****. Надійність технічних систем / Під ред. І.А.Ушакова. -М.: 1985.* ***9.*** *Романов А. И. Телекоммуникационные сети и управление. – К.: ИПЦ „Киевский университет", 2003. – 247 с.* ***10.*** *Антонов А. В., Нікулін М. С. Статистичні моделі в теорії надійності. М.: Абрис: 2012.* ***11.*** *Рябінін І. А. Надійність і безпека структурно-складних систем. СПб.: Видавництво Санкт-Петербурзького університету, 2007 р., 278 с.*

***Анна Чунарьова, Руслана Зюбіна***
*Національний авіаційний університет*

**УДК 004.056.53(045)**

# НОВІТНІ МЕТОДИ АУТЕНТИФІКАЦІЇ В БЕЗДРОТОВИХ СИСТЕМАХ ТА МЕРЕЖАХ

*Анотація:* **Проведено аналіз стандартів автентифікації в сучасних бездротових мережах. Розроблено рекомендації щодо використання новітніх методів аутентифікації користувачів в сучасних бездротових мережах та запропонована множина захисних функцій автентифікації на еліптичних кривих.**

*Summary:* **The analysis of authentication standards in modern wireless networks. The recommendations on the use of new methods of user authentication in wireless networks and proposed a variety of protective functions authentication basic on elliptic curves.**

*Ключові слова:* **Аутентифікація, ідентифікація, еліптична крива, бездротові мережі, криптосистеми.**

## І Вступ

Захист інформаційних ресурсів є базовим чинником процесу проектування будь-яких інформаційних систем незалежно від виду комутації (дротові або бездротові мережі). Розробка політики безпеки, процедури формування моделей порушників, а також методи захисту інформаційних ресурсів мають будуватись на однакових засадах як для дротових, так і для бездротових мереж. Однак існують певні організаційно-технічні відмінності даних процесів.

Базовою відмінністю бездротових систем та мереж (БСМ) є використання частотного ресурсу для передачі інформаційних потоків даних від джерела повідомлення до користувача з урахуванням територіального рознесення об'єктів. Сам принцип бездротової передачі даних включає в себе можливість несанкціонованого підключення як до вузлів передачі, так і до джерел інформації. Безпека бездротових мереж включає в себе два аспекти: захист від несанкціонованого доступу та шифрування інформаційних потоків. У даному випадку розширюється клас можливих загроз інформаційним ресурсам та послугам системи.

Значний відсоток загроз інформаційним ресурсам БСМ становлять загрози, що пов'язані із системою управління доступом. Впровадження правил розмежування доступу до інформаційних ресурсів бездротової мережі пояснюється масовістю використання бездротових технологій. Адже відсутність дротів – це, перш за все, мобільність та масштабованість локальної обчислювальної мережі (ЛОМ). Проте використання радіодіапазону збільшує ймовірність порушення атрибутів конфіденційності, цілісності та доступності оброблюваної інформації. Тому використання автентифікації для захисту інформаційних ресурсів є досить актуальною задачею з точки зору забезпечення розмежування прав доступу.

## II Постановка задачі

Розробка, дослідження і розвиток ефективних методів автентифікації користувачів та інформаційних ресурсів в бездротових мережах із використанням криптографічних перетворень, що забезпечують комплексний підхід до організації правил розмежування доступу, протоколів мережевої автентифікації на основі Extensible Authentication Protocol (EAP), використання серверів автентифікації та організація захищених каналів обміну персональними даними, а також створення відповідних програмних засобів здійснення автентифікації та авторизації є актуальною науково-технічною задачею та розглядається в даній статті. Застосування криптографічних методів і засобів з метою забезпечення цілісності та конфіденційності інформаційних ресурсів БСМ є звичайною процедурою для всіх типів інформаційних систем.

**Метою даною статті** є розробка рекомендацій щодо використання новітніх методів автентифікації користувачів на основі підвищення ефективності функціонування сучасних БСМ.

## III Основна частина

**Аналіз сучасних методів автентифікації в бездротових мережах на основі стандарту IEEE 802.11**

Одним із рубежів безпеки в бездротових мережах є ідентифікація та автентифікація користувачів. Відповідно до стандарту IEEE 802.11 існує три базових режими безпеки, що вибираються бездротовим пристроєм залежно від рівня секретності:

– відкритий режим (шифрування та автентифікація не використовується);

– захищений режим без автентифікації, але з шифруванням трафіку;

– захищений режим з автентифікацією і шифруванням трафіку.

Основними стандартами автентифікації в бездротових мережах є стандарти IEEE 802.11, WPA, WPA2 та IEEE 802.1x. Стандартний механізм реалізації мережної безпеки (Traditional Security Network), заснований на впровадженні процесів автентифікації користувачів інформаційних ресурсів та послуг бездротових мереж з урахуванням відкритого типу автентифікації (Open Authentication) та процедури автентифікації зі спільним ключем (Shared Key Authentication), не здатний забезпечити захист від зовнішніх атак з боку зловмисника [1].

Відкрита автентифікація не дозволяє точці радіодоступу визначити чи є абонент легітимним, а автентифікація зі спільним ключем потребує налаштувань у абонента статичного ключа шифрування. Оскільки у БСМ постійно проходить обмін фреймами, що містять ключ шифрування, то механізм автентифікації з відкритим ключем не захищений від атак зі сторони спостерігача (Man in the middle attack).

При побудові системи захисту інформаційних ресурсів бездротових мереж широке використання набули два інших механізми автентифікації, що формуються на ідентифікації технічних характеристик конкретизованої бездротової мережі та ідентифікації користувача визначеної мережі. Даний механізм захисту інформації засновано на:

– генерації та використанні ідентифікатора конкретної БСМ мережі (Service Set Identifier –SSID);

– автентифікації користувачів мережі за визначеними ресурсами системи – MAC-адресами (MAC Address Authentication).

Ідентифікатори SSID регулярно передаються між точками доступу у фреймах Beacon, що виконують лише інформаційну роль у радіомережі. Тобто дані, що містяться у SSID, передаються у відкритому вигляді, що не може гарантувати безпеку БСМ від зовнішніх загроз.

Що ж стосується MAC-адрес, то стандарт IEEE 802.11 потребує їх передачі у відкритому вигляді. В результаті в БСМ, що використовує механізм автентифікації за MAC-адресами, зловмисник може обійти автентифікацію шляхом підміни своєї MAC-адреси легітимною.

*Стандарт IEEE 802.11 з традиційною безпекою*

Стандарт IEEE 802.11 з традиційною безпекою (Traditional Security Network – TSN) передбачає два механізми автентифікації бездротових абонентів:

– відкриту автентифікацію (Open Authentication);

– автентифікацію зі спільним ключем (Shared Key Authentication).

Як засіб автентифікації у бездротових мережах широко застосовується два інших механізми, що виходять

за рамки стандарту IEEE 802.11, а саме використання ідентифікаторів бездротової локальної мережі (Service Set Identifier – SSID) та автентифікація абонента за його MAC- адресою (MAC Address Authentication).

SSID представляє собою атрибут бездротової мережі, що дозволяє логічно відрізняти мережі одну від іншої. В загальному випадку абонент бездротової мережі повинен задати у себе відповідний SSID для того, щоб отримати доступ до потрібної локальної мережі. Проте SSID ніяк не забезпечує конфіденційність інформаційних ресурсів та не забезпечує автентифікацію абонента відносно точки доступу (Access Point – AP) бездротової мережі [1].

*Принцип автентифікації абонента в IEEE 802.11*

Автентифікація в стандарті IEEE 802.11 орієнтована на автентифікацію абонентського пристрою, а не конкретного абонента як користувача мережевих ресурсів. Процес автентифікації абонента бездротової локальної мережі IEEE 802.11 складається із наступних етапів:

1. Абонент (Client) відправляє фрейм Probe Request в усі радіоканали;
2. Кожна точка радіодоступу, в зоні радіобачення якої знаходиться абонент, відправляє у відповідь фрейм Probe Response.
3. Абонент вибирає найкращу для нього точку доступу і відправляє в обслуговуваний нею радіоканал запит на автентифікацію (Authentication Request).
4. Точка доступу відправляє підтвердження автентифікації (Authentication Reply).
5. У випадку успішної автентифікації абонент відправляє точці доступу фрейм асоціації (Association Request).
6. Точка доступу відправляє у відповідь фрейм підтвердження асоціації (Association Response).

*Відкрита автентифікація (Open System Authentication – OSA)*

Відкрита автентифікація по суті не є алгоритмом автентифікації в первинному розумінні. В процесі відкритої автентифікації відбувається обмін повідомленнями двох типів:

– запит автентифікації (Authentication Request);

– підтвердження автентифікації (Authentication Response).

Таким чином, при відкритій автентифікації можливий доступ будь-якого абонента до бездротової локальної мережі. Якщо в бездротовій мережі не використовується шифрування, будь-який абонент, що знає ідентифікатор SSID точки радіо доступу, отримає доступ до мережі. При використанні точками доступу шифрування WEP самі ключі шифрування стають засобом контролю доступу. Якщо абонент не володіє коректним WEP-ключем, то навіть у випадку успішної автентифікації він не зможе ні передавати дані через точку доступу, ні розшифрувати дані, що передані точкою доступу.

*Автентифікація зі спільним ключем*

Автентифікація зі спільним ключем є другим методом автентифікації стандарту IEEE 802.11. Автентифікація зі спільним ключем потребує налаштувань у абонента статичного ключа шифрування WEP і складається з наступних етапів:

1. Абонент відправляє точці доступу запит автентифікації, вказуючи при цьому необхідність використання режиму автентифікації зі спільним ключем.
2. Точка радіодоступу відправляє підтвердження автентифікації, що містить Challenge Text.
3. Абонент шифрує Challenge Text своїм статичним WEP-ключем і відправляє точці доступу запит асоціювання.
4. Якщо точка радіо доступу в стані успішно розшифрувати запит асоціювання і Challenge Text, що міститься в ньому, вона відправляє абоненту підтвердження асоціювання і таким чином надає доступ до мережі [2].

*Автентифікація за MAC-адресами*

Автентифікація абонента за його MAC-адресою не передбачена стандартом IEEE 802.11, проте підтримується багатьма виробниками обладнання для бездротових мереж. При автентифікації за MAC-адресою відбувається порівняння MAC-адреси абонента або із локальним списком дозволених адрес легітимних абонентів, або за допомогою зовнішнього серверу автентифікації. Автентифікація за MAC-адресою використовується як доповнення до відкритої автентифікації та автентифікації зі спільним ключем стандарту IEEE 802.11 для зменшення ймовірності доступу сторонніх об'єктів [3].

**Стандарт IEEE 802.1x/EAP**

Проблеми, з якими зіштовхнулись розробники та користувачі мереж на основі стандарту IEEE 802.11, примусили шукати нове рішення захисту бездротових мереж. Тоді були виявлені компоненти, що впливають на систему безпеки бездротової локальної мережі:

1. архітектура автентифікації;
2. механізм автентифікації;
3. механізм забезпечення конфіденційності та цілісності даних.

Стандарт IEEE 802.1x описує єдину архітектуру контролю доступу до портів із використанням різноманітних методів автенифікації абонентів.

Розширюваний протокол автентифікації (Extensible Authentication Protocol – EAP) підтримує централізовану автентифікацію елементів інфраструктури бездротової мережі та її користувачів з можливістю динамічної генерації ключів шифрування [4].

*Архітектура та механізм автентифікації IEEE 802.1x*

Стандарт IEEE 802.1x розроблявся для того, щоб забезпечити автентифікацію користувачів на канальному рівні моделі OSI в комутованих дротових мережах. Алгоритми автентифікації стандарту 802.1x можуть забезпечити клієнта динамічними, орієнтованими на користувача ключами.

Архітектура IEEE 802.1x включає наступні обов'язкові логічні елементи:

- Клієнт (Supplicant) – знаходиться в ОС абонента;
- Автентифікатор (Authenticator) – знаходиться в ПЗ точки доступу;
- Сервер автентифікації (Authentication Server).

IEEE 802.1x надає абоненту бездротової локальної мережі лише засоби передачі атрибутів серверу автентифікації та допускає використання різноманітних методів та алгоритмів автентифікації. Задача серверу автентифікації – підтримка дозволених політикою мережевої безпеки методів автентифікації.

Автентифікатор, знаходячись у точці доступу, створює логічний порт для кожного клієнта на основі його ідентифікатора асоціювання. Логічний порт має два канали обміну даними. Неконтрольований канал безперешкодно пропускає трафік із бездротового сегменту мережі у дротовий і навпаки, в той час як контрольований канал потребує успішної автентифікації для проходження фреймів.

Для можливості доступу до інформаційних ресурсів бездротової мережі клієнт асоціюється із точкою радіодоступу. Автентифікатор розпізнає факт підключення до точки доступу і активує логічний порт для клієнта, одразу переводячи його в стан «неавторизований». В результаті через клієнтський порт можливий лише обмін трафіком протоколу IEEE 802.1x, для всіх інших даних порт заблокований. Клієнт також може відправити повідомлення EAP Start (початок EAP- автентифікації) для запуску процесу автентифікації.

Автентифікатор відправляє повідомлення EAP Request Identity (запит імені EAP) та очікує від клієнта його ім'я (Identity). Відповідь клієнта EAP Response, що містить необхідні атрибути, перенаправляється серверу автентифікації.

Після завершення автентифікації сервер відправляє повідомлення RADIUS-ACCEPT (прийняти) або RADIUS-REJECT (відхилити) автентифікатору. При отриманні повідомлення про успішне завершення автентифікації автентифікатор переводить клієнта у стан «авторизований», після чого починається передача всіх даних абонента.

*Extensible Authentication Protocol (EAP)*

У стандарті 802.1x, як уже зазначалося, автентифікація користувачів на канальному рівні виконується за протоколом EAP, що був розроблений Групою з проблем проектування Intrnet (IETF).

EAP є «узагальненим» протоколом в системі автентифікації, авторизації та обліку (Authentication Authorization and Accounting – AAA), що забезпечує роботу різноманітних методів автенифікації. Сервер доступу, в ролі якого виступає Wireless Access Point, тунелює повідомлення протоколу автентифікації, що циркулюють між абонентом та сервером автентифікації [5, 6].

Загальним недоліком методів автентифікації стандарту IEEE 802.11 є передача службової інформації у відкритому вигляді через незахищені канали передачі даних. Винятком є стандарт IEEE 802.1x, що підтримує автентифікацію елементів інфраструктури БСМ з можливістю динамічної генерації ключів шифрування. Автентифікація у БСМ на основі IEEE 802.1x регламентується розширюваним протоколом автентифікації EAP. Відповідно до вказаних проблем, доцільно використовувати стійкі криптографічні алгоритми для проведення процедури автентифікації та як обов'язкового елемента в системі управління доступом. Але, в свою чергу, використання криптографічних перетворень не повинно знижувати пропускної здатності бездротових каналів передачі даних.

Одним із таких методів є криптографічні перетворення із використанням еліптичних кривих, що, порівняно з задачею факторизації числа, що використовується в RSA, або з задачею цілочислового логарифмування, що використовується в алгоритмі Діффі-Хеллмана та в DSS (Digital Signature Standard), забезпечує еквівалентний захист при меншій довжині ключа.

**Процедура аутентифікації на базі еліптичних кривих**

Еліптична криптографія – розділ криптографії, що вивчає асиметричні криптосистеми, основою яких є еліптичні криві над скінченними полями.

Еліптичні криві широко використовуються для побудови криптосистем з відкритим ключем. Це пояснюється наступною низкою причин.

1. Еліптичні криві забезпечують максимально можливу для криптосистем з відкритим ключем стійкість

на один біт розміру задачі.

2. Еліптичні криві дозволяють реалізувати широкий спектр криптографічних функцій (шифрування з відкритим ключем, автентифікацію на основі діалогових та бездіалогових доказів з нульовим розголошенням знань і т. д.). Криптографічні перетворення на базі еліптичних кривих використовуються як основа російського (ГОСТ Р 34.10-2001) та американського (Elliptic Curve Digital Signature Algorithm – ECDSS) стандартів ЕЦП.

3. Еліптичні криві забезпечують практично нульову швидкість падіння стійкості з часом, що дозволяє зберегти розмір задачі. Наприклад, у криптосистемах, основою яких є логарифмування в скінченному полі або розкладання чисел на множники, розмір задачі потрібно подвоювати приблизно кожні 5 років.

4. Криптосистеми з відкритим ключем не еліптичних кривих дозволяють виконувати незалежну зміну особистих ключів в інформаційній системі. В криптосистемах, основою яких є логарифмування в скінченному полі, це не так. Найкращий метод логарифмування (решітка числового поля) припускає створення бази даних для даної характеристики поля, за допомогою якої логарифми швидко обчислюються. Тому зміна особистого ключа практично не дозволяє збільшити строк його служби, необхідно змінювати характеристику поля та всі особисті ключі.

Ключ, побудований на еліптичній кривій над скінченним полем, забезпечує криптостійкість алгоритму, еквівалентну ключу втричі більшої довжини над полем цілих чисел.

Криптоалгоритм заснований на «Проблемі Дискретного Логарифму Еліптичної Кривої» (Elliptic Curve Discrete Logarithm Problem – ECDLP): «Дано: «базова точка» $Q$ та розташована на кривій точка $P = kQ$; Знайти: $k$». Для еліптичних кривих та базових точок розв'язок таких рівнянь являє доволі велику складність. Оцінку складності $S$ цієї задачі в загальному випадку прийнято визначати за допомогою алгоритму Полларда: $S = O(\sqrt{r})$, де $r$ – порядок групи точок еліптичної кривої, який не може бути покращений за рахунок збільшення об'єму пам'яті та не допускає ефективного розпаралелювання.

З точки зору криптографії є можливість визначити нову криптографічну систему на основі еліптичних кривих. Через складність зламування алгоритм ECDLP можна застосовувати для побудови «абсолютно» криптостійких систем; забезпечуючи еквівалентний рівень безпеки, алгоритм має значно менший розмір ключа ніж, наприклад, алгоритми RSA або DSA. В Табл. 1 порівнюються приблизні розміри параметрів еліптичних криптосистем та RSA, що забезпечують однакову стійкість шифру, яка розраховується на основі сучасних методів розв'язку ECDLP та факторизації (пошуку дільників) для великих цілих чисел.

Таблиця 1 – Порівняння параметрів еліптичних криптосистем та RSA

| **Система на еліптичних кривих (базова точка *P*)** | **Система RSA (довжина модуля *n*)** |
|---|---|
| 106 біт | 512 біт |
| 132 біт | 768 біт |
| 160 біт | 1024 біт |
| 224 біт | 2048 біт |

Основна перевага еліптичної криптографії полягає в тому, що наразі невідомо субекспонентних алгоритмів для вирішення задачі дискретного логарифмування в групах точок еліптичної кривої. Використання ключів малих розмірів знижує вимоги до обчислювальних потужностей порівняно з вимогами систем на основі RSA. В Табл. 2 приведені порівняльні характеристики алгоритмів RSA та ECDSA (Elliptic Curve Digital Signature Algorithm) при створенні та перевірці ЕЦП (Електронний Цифровий Підпис). Обидва алгоритми виконувались на паралельних процесорах Motorola 56303 DSP з тактовою частотою 66 МГц.

Таблиця 2 – Порівняльні характеристики алгоритмів RSA і ECDSA

| **Крипто-алгоритми** | **Створення підпису** | **Перевірка підпису** |
|---|---|---|
| **RSA (1024 біт)** | 25 мс | 1 мс |
| **ECDSA (160 біт)** | 32 мс | 33 мс |
| **RSA (2048 біт)** | 120 мс | 5 мс |
| **ECDSA (216 біт)** | 68 мс | 70 с |

Криптосистеми на основі еліптичних кривих отримують все більше поширення скоріше як альтернатива, а не заміна системам на основі RSA, оскільки системи на основі ECDLP мають деякі переваги, особливо при

використанні в пристроях із малопотужними процесорами та малим об'ємом оперативної пам'яті. Таким чином, криптосистеми на основі еліптичних кривих можна з успіхом використовувати в бездротових мережах передачі даних, де критичними є вимоги до обчислювальних потужностей та пропускної здатності каналу передачі.

**Множина захисних функцій автентифікації на еліптичних кривих**

Найважливішою частиною підсистеми автентифікації є сукупність алгоритмів автентифікації, що задають множину захисних функцій, які визначають, що та при яких умовах може бути захищено. Доведено, що захисні функції утворюють решітку, що ізоморфна підрешітці булевих функцій [7].

Таблиця 3 – Впорядкованість захисних функцій автентифікації

| **Координати захисних функцій** | **Впорядкованість** |
|---|---|
| Тип автентифікації | Автентифікація повідомлення $\supseteq$ Упізнання |
| Число сеансів на одному ключі | Багаторазова автентифікація $\supseteq$ Одноразова автентифікація |
| Тип використовуваного каналу зв'язку (можливість діалогу) | Бездіалогова автентифікація $\supseteq$ Діалогова автентифікація |
| Ступінь довіри до верифікатора | Недовірений верифікатор $\supseteq$ Довірений верифікатор |
| Якість зв'язку (при одноразовій автентифікації необхідна надійність при обміні інформацією) | Некритичність надійного обміну інформацією $\supseteq$ Необхідність надійного обміну інформацією |
| Наявність служби єдиного часу (необхідна для захисту від повторів або затримок інформації при бездіалоговій автентифікації | Необов'язковість єдиного часу $\supseteq$ Наявність єдиного часу |
| Відносний об'єм переданої службової інформації (відношення об'єму переданих даних до ентропії $H_k(k \mid k')$) | Менший відносний об'єм службової інформації $\supseteq$ Більший відносний об'єм службової інформації |

Якщо в підсистемі автентифікації як математичну структуру використовувати групу точок еліптичної кривої над простим полем, то як параметр підсистеми можуть виступати, наприклад, скінченне поле, рівняння еліптичної кривої та порядок групи, для визначення якого достатньо знайти число точок кривої [8].

## IV Висновки

Проведено аналіз стандартів автентифікації в сучасних бездротових мережах. На основі проведеного аналізу розроблено рекомендації щодо використання новітніх методів аутентифікації користувачів в сучасних БСМ та запропонована множина захисних функцій автентифікації на еліптичних кривих.

*Список використаної літератури:* ***1.*** *Педжман Р. Основы построения беспроводных локальных сетей стандарта 802.11 / Педжман Р., Джонатан Л. – М.: Издательский дом «Вильямс», 2004. – 304 с.* ***2.*** *Беспроводные сети Wi-Fi / [Пролетарский А. В., Баскаков И. В., Чирков Д. Н. и др.]. – М.: БИНОМ. Лаборатория знаний, 2007. – 216 с.* ***3.*** *Yongliang L., Gao W., Yao H., Yu X. Elliptic Curve Cryptography Based Wireless Authentication Protocol, International Journal of Network Security 5, no. 3, 2007.* ***4.*** *Шахнович И. В. Современные технологии беспроводной связи. – М.: Техносфера, 2006. – 285 с.* ***5.*** *Гейер Д. Беспроводные сети. Первый шаг. – М.: Издательский дом «Вильямс», 2005. – 189 с.* ***6.*** *Максим М. Безопасность беспроводных сетей / Максим М., Полино Д. – М.: Компания АйТи; ДМК Пресс, 2004. – 288 с.* ***7.*** *Muller V. Fast Multiplication on Elliptic Curve over Small Field of Characteristic Two, Journal of Cryptography 11, no. 2, 1998.* ***8.*** *Washington L. C. Elliptic curves Number Theory and Cryptography. – Chapman & Hall / CRC, 2003.*