МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учреждение образования «БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ

ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Факультет информационных технологий

Кафедра информационных систем и технологий

Специальность Информационные системы и технологии

ОТЧЕТ ПО ЛАБОРАТОРНОЙ РАБОТЕ №10 НА ТЕМУ:

Исследование алгоритмов генерации и верификации электронной цифровой подписи

Выполнила:

Студентка 3 курса 1 группы ФИТ

Шимчёнок Елизавета Константиновна

**Цель:** изучение алгоритмов генерации и верификации ЭЦП и приобретение практических навыков их реализации.

**Задачи:**

1. Закрепить теоретические знания по алгебраическому описанию и алгоритмам реализации операций вычисления однонаправленных хеш-функций.
2. Освоить методику оценки криптостойкости хеш-преобразований на основе «парадокса дня рождения».
3. Разработать приложение для реализации заданного алгоритма хеширования (из семейств MD и SHA).
4. Оценить скорость вычисления кодов хеш-функций.
5. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**Теоретические сведения**

Электронная цифровая подпись – контрольная характеристика сообщения, которая вырабатывается с использованием личного ключа, проверяется с использованием открытого ключа, служит для контроля целостности и подлинности сообщения и обеспечивает невозможность отказа от авторства.

Таким образом, ЭЦП выполняет те же функции, что и собственноручная (поставленная «от руки») подпись:

– аутентифицирование лица, подписавшего сообщение;

– контроль целостности подписанного сообщения;

– защита сообщения от подделок;

– доказательство авторства лица, подписавшего сообщение, если это лицо отрицает свое авторство.

Важнейшие отличительные особенности ЭЦП:

– ЭЦП представляет собой бинарную последовательность (в отличие от графического образа, каковым является подпись от руки);

– указанная бинарная последовательность зависит от содержания подписываемого сообщения.

Принадлежность ключа, в предположении, что он известен только законным пользователям, позволяет решать все «возложенные на ЭЦП», сформированную на основе этого ключа, задачи. В соответствии с этим обстоятельством перечисленные выше функции ЭЦП могут быть реализованы на основе классических методов зашифрования/расшифрования:

– на основе симметричных систем (с тайным ключом);

– на основе симметричных систем и посредника;

– на основе асимметричных систем (с открытым ключом).

Классическая технология использования ЭЦП предусматривает подписание не самого сообщения (обозначим его здесь M0), а его хеша, H(M0), что позволяет:

– сокращает время генерации/верификации подписи;

– снизить вероятность ошибок в итоговом документе.

Общая структура подписанного документа – M0 – M' – представляет конкатенацию этого документа и ЭЦП *S*. И еще может конкатенироваться служебная информация (дата, время отправки, информация об отправителе).

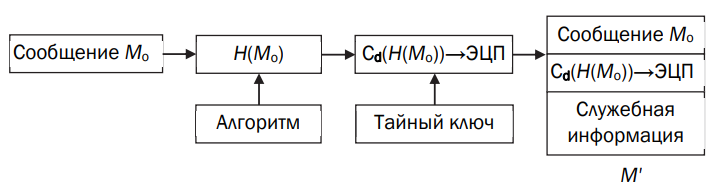


Рисунок 1 – Пояснение к процедуре формирования ЭЦП и структуре подписанного документа

Важное свойство цифровой подписи: её может проверить каждый, кто имеет доступ к открытому ключу её автора.

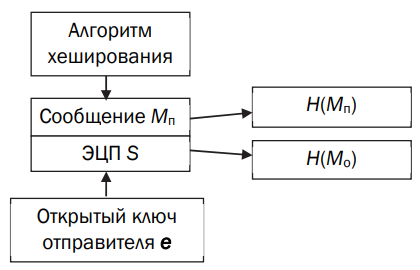


Рисунок 2 – Общий вид процедуры верификации ЭЦП (без учета использования служебной информации)

Если H(Mп)=H(M0) – подпись подлинная и документ целостный, что значит, что Mп=M0, где Mп – полученный документ, M0 – исходный документ.

При генерации ЭЦП (по классической схеме) для сообщения М отправитель последовательно выполняет следующие действия:

– вычисляет хеш (хеш-образ) сообщения *М*: *Н*(*М*);

– вычисляет содержание ЭЦП (собственно ЭЦП S) по хешу Н(М) с использованием своего закрытого ключа d: S =Cd (Н(М));

– присоединяет (конкатенирует) ЭЦП к сообщению М и некоторой служебной информации, создавая таким образом итоговое сообщение *М'*;

–  посылает сообщение *М'* получателю.

Получив сообщение *М'*, другая сторона последовательно выполняет следующие действия:

– отделяет цифровую подпись S от сообщения М (для общего случая применим одинаковые символьные обозначения);

– применяет к сообщению М операцию хеширования, используя ту же функцию, что и отправитель, и получает хеш-образ полученного сообщения;

– используя открытый ключ отправителя, расшифровывает S, т. е. извлекает из ЭЦП хеш-образ отправленного сообщения;

– проверяет соответствие (равенство) обоих хеш-образов, и если они совпадают, то отправитель действительно является тем, за кого себя выдает, а сообщение при передаче не подверглось искажению.

Необходимо, чтобы вычисление легитимной подписи без знания закрытого ключа было вычислительно сложным процессом.

**Ход работы**

Было разработано приложение в соответствии с задачами:

– генерация и верификация ЭЦП на основе алгоритмов RSA, Эль-Гамаля и Шнорра;

– оценка времени выполнения указанных процедур при реальных (требуемых) ключевых параметрах.

**Алгоритм RSA**

Алгоритм генерации подписи заключается в следующих операциях:

– выбор простых чисел p, q;

– выбор случайного числа e, взаимно простого с функцией Эйлера ф(n)=(p-1)(q-1);

– нахождение числа d, такого что ed = 1 mod ф(n);

– вычисление хеш-образа сообщения h=H(M);

– вычисление ЭЦП:

S = hd mod n.

Далее полученный открытый ключ {e, n} и письмо с ЭЦП {M, S} будут отправлены получателю.

Результат работы приложения представлен на рисунке 3. На консоль выводятся все значения, которые были заданы изначально или вычислены в ходе работы программы.

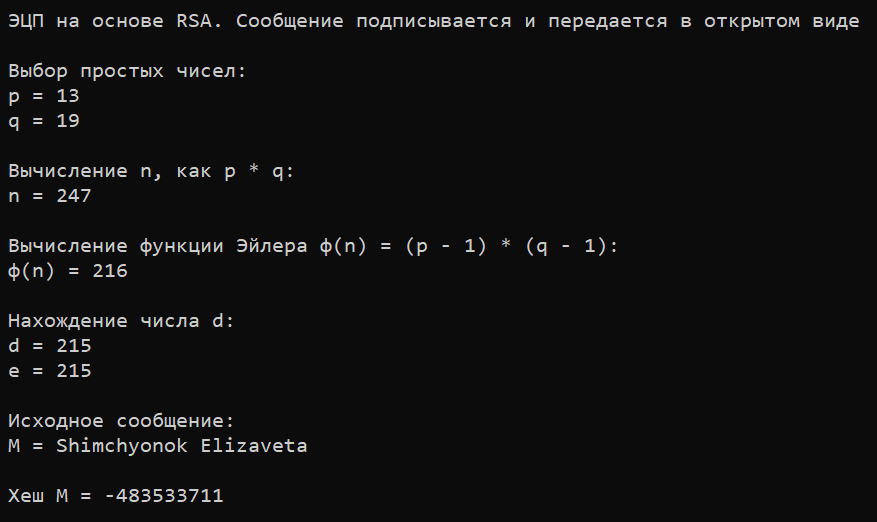


Рисунок 3 – Результат работы алгоритма RSA

Сообщение М заполняется текстом из файла. Содержание файла изображено на рисунке 4.

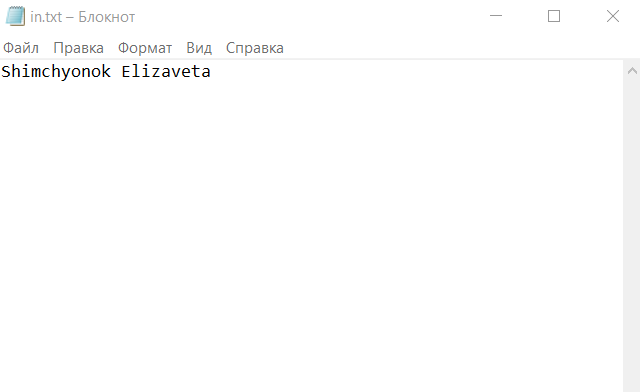


Рисунок 4 – Содержание текстового файла

Далее требуется провести верификацию данного файла, чтобы проверить его подлинность. Для этого необходимо выполнить следующие действия:

– вычислить h = H(Mп) = Se mod n;

– сравнить значение выше с полученным H(M);

Если полученные значения совпали, подпись верифицирована.

На рисунке 5 продемонстрировано следующее: сообщение М соответствует содержанию файла. Программа проверила хэш электронной подписи и хэш файла и сравнила их. В результате файл оказался подлинным.

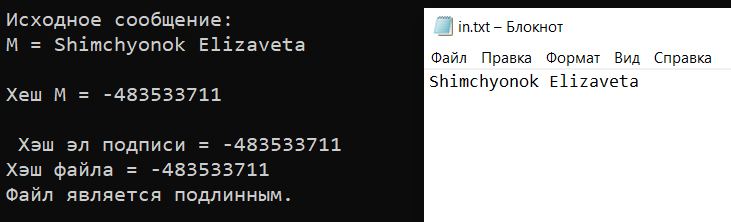


Рисунок 5 – Результат верификации

Далее файл был модифицирован с целью проверить правильность работы приложения. Результат изображен на рисунке 6.

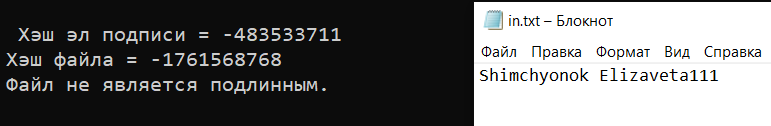


Рисунок 6 – Работа программы в случае с измененным исходным файлом

Таким образом, если целостность документа нарушена, то хеш будет изменен, а соответственно и подтвердить подлинность файла не получится.

В случае, если подписываемое сообщение должно передаваться в зашифрованном виде, то M’ зашифровывается при помощи открытого ключа получателя, а расшифровывается закрытым ключом получателя (как обычно) перед процессом верификации.

Время зашифровки в среднем составляет 25 мс, тогда как время расшифровки занимает 154 мс – в 6 раз дольше.

**Алгоритм Эль-Гамаля**

Алгоритм генерации подписи заключается в следующих операциях:

* выбор простого числа p;
* вычисление g, причем g<p – первообразный корень по модулю p;
* выбор x, меньшего p;
* вычисление y = gx mod p.

В результате зашифрования сообщения с ЭЦП на выходе будет лишь одна пара чисел, не для каждого блока сообщения.

Далее необходимо проделать следующие операции:

* выбрать k – взаимно простое число с (p-1);
* вычислить a = gk mod p;
* вычислить b = k-1 (H(Mo) - xa) mod (p-1);

Пара чисел S = {a,b} и будет являться цифровой подписью. Далее получателю будет отправлено сообщение M’=M0||S, которое является конкатенацией исходного сообщения и ЭЦП.

Для верификации подлинности полученного сообщения необходимо проверить равенство

ya \* ab (mod p) = gh (mod p),

в которое подставляются все вычисленные ранее значения, h=H(Mп) – хеш-образ полученного сообщения.

Если данное равенство выполняется, подпись верифицирована и подлинна.

Протестируем приложение, запустив его. Результат в консоли представлен на рисунке 7. Изначально на консоль выводятся все значения, которые мы задавали самостоятельно или которые были вычислены в ходе рботы приложения. Далее выводится значения ЭЦП и результат проверки.

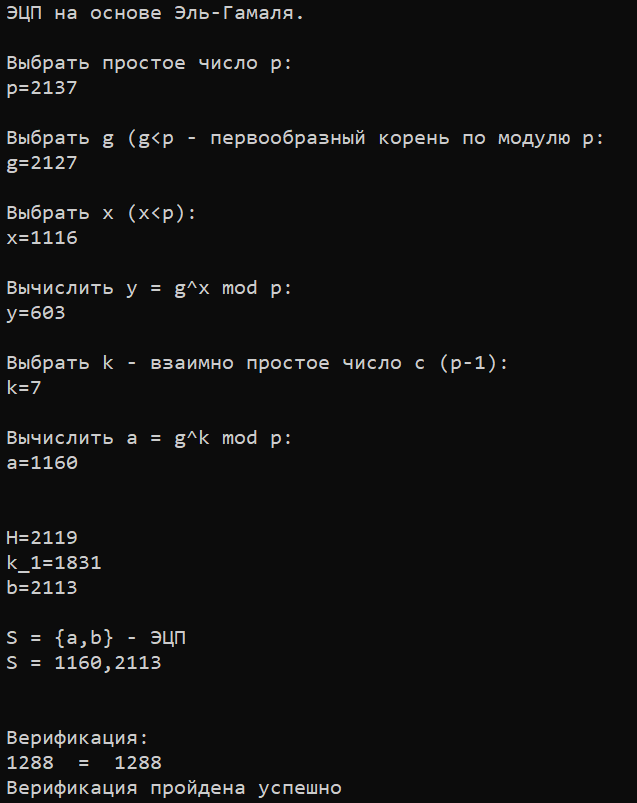


Рисунок 7 – Результат работы алгоритма Эль-Гамаля

Генерация ЭЦП и верификация занимают некоторое время (рисунок 8).

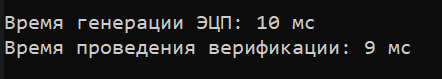


Рисунок 8 – Замер времени выполнения задач

**Алгоритм Шнорра**

Схема Шнорра является основой стандарта ЭЦП в Беларуси.

Одной из особенностей ЭЦП Эль-Гамаля является то, что число p должно быть очень большим, чтобы сделать действительно трудной проблему дискретного логарифма. Рекомендуется длина p, по крайней мере, должна составлять 1024 бита. Чтобы уменьшить размер подписи, Шнорр предложил новую схему, но с уменьшенным размером подписи.

Алгоритм генерации ключевой информации заключается в следующих шагах (рисунок 9):

– генерация простых чисел p, q;

– вычисление q = (p-1) – делителя;

– выбор любого g≠1, такого что gq = 1 mod p;

– выбор любого числа х<q – это и будет закрытый ключ;

– вычисление y = g–X mod p.

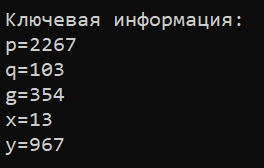


Рисунок 9 – Генерация ключевой информации

Сообщение, пересылаемое от отправителя получателю ­– Shimchyonok Elizaveta.

Для подписи сообщения необходимо реализовать следующий алгоритм (рисунок 10):

– выбор случайного числа 1 < k < q;

– вычислить параметр a = gk mod p;

– создать хеш-образ сообщения: h = H(Mo||a);

– вычислить b = (k+xh) mod q;

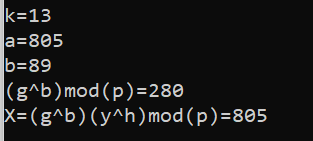


Рисунок 10 – Генерация параметров для осуществения подписи документа

Получателю будет отправлено сообщение M’ = Mo||S, являющееся конкатенацией исходного сообщения и ЭЦП S={h,b}.

Для проверки подписи на подлинность необходимо вычислить

X = gb \* yh (mod p),

после чего проверить выполняется ли равенство вычисленного ранее h хеш-образа и H(Мп||X) хеш-образа конкатенации полученного сообщения с вычисленным значением Х. Если равенство выполняется, подпись верифицирована (рисунок 11).

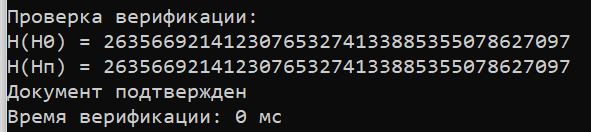


Рисунок 11 – Процесс верификации

Время генерации ЭЦП занимает больше времени (8 мс), нежели процесс верификации (1 мс).

**Ответы на вопросы**

1. Дать определение ЭЦП.

Электронная цифровая подпись – бинарная (или в ином виде) последовательность символов, являющаяся реквизитом электронного документа, зависящая от содержания этого документа и предназначенная для подтверждения целостности и подлинности электронного документа.

1. Охарактеризовать основные функции ЭЦП.

* подтверждение подлинности;
* обеспечение целостности данных;
* неотказуемость;
* ­ конфиденциальность;
* недвусмысленность.

1. В чем заключаются сходства и различия между собственноручной и электронной подписью?

Сходства:

– подтверждают авторство документа или сообщения;

– могут иметь юридическую силу.

Различия:

– Собственноручная подпись создается физически с использованием ручки или пера на бумажном документе. Электронная подпись, напротив, представляет собой цифровой код или криптографическую конструкцию, которая связывается с электронным документом или сообщением.

– Собственноручная подпись создается физически путем ручного написания или подписывания документа. Электронная подпись создается с использованием криптографических алгоритмов и публичных и приватных ключей.

– Собственноручная подпись применима только к бумажным документам, в то время как электронная подпись используется для электронных документов и сообщений, которые могут быть переданы через сети и хранены в цифровом формате.

– Электронная подпись может быть связана с сертификатом, выданным доверенным центром сертификации, который подтверждает идентификацию подписывающего лица. Собственноручная подпись не имеет такого механизма удостоверения.

1. Охарактеризовать основные способы реализации ЭЦП.

В соответствии с этим обстоятельством перечисленные выше функции ЭЦП могут быть реализованы на основе классических методов зашифрования/расшифрования:

– на основе симметричных систем (с тайным ключом);

– на основе симметричных систем и посредника;

– на основе асимметричных систем (с открытым ключом).

1. Имеется ли различие в использовании ключевой информации при передаче зашифрованных сообщений и при передаче подписанных (ЭЦП) сообщений?

Да, есть различие в использовании ключевой информации при передаче зашифрованных сообщений и при передаче подписанных сообщений с использованием электронной цифровой подписи (ЭЦП).

При передаче зашифрованных сообщений используются симметричные или асимметричные криптографические алгоритмы, где отправитель и получатель используют общий секретный ключ или публичный ключ получателя для зашифрования и расшифрования сообщения. Это обеспечивает конфиденциальность данных, так как только получатель, обладающий соответствующим ключом, может расшифровать сообщение.

При передаче подписанных сообщений с использованием ЭЦП используются асимметричные криптографические алгоритмы. Отправитель создает цифровую подпись, используя свой приватный ключ, и прикрепляет ее к сообщению. Получатель проверяет подпись с использованием публичного ключа отправителя. Это обеспечивает подлинность и целостность данных, так как подпись связана с конкретным отправителем и не может быть подделана или изменена без обнаружения.

Таким образом, в случае зашифрованных сообщений используются ключи для обеспечения конфиденциальности данных, а в случае подписанных сообщений с помощью ЭЦП ключи используются для обеспечения подлинности и целостности данных.

1. Охарактеризовать криптостойкость ЭЦП на основе RSA, схемы Эль-Гамаля, схемы Шнорра, а также на основе DSA.

RSA (Rivest-Shamir-Adleman) – это асимметричный алгоритм, основанный на сложности факторизации больших простых чисел. Криптостойкость RSA основана на трудности факторизации больших чисел на простые множители. Чем больше размерность ключа (длина числа), тем сложнее выполнить факторизацию и взломать RSA. RSA считается криптостойким при использовании достаточно длинных ключей (например, 2048 бит и более).

Схема Эль-Гамаля основана на сложности вычисления дискретного логарифма в конечных полях. Криптостойкость схемы Эль-Гамаля также основана на сложности вычисления дискретного логарифма, и ее безопасность зависит от выбранной группы и размерности ключей. Для обеспечения криптостойкости схемы Эль-Гамаля необходимо выбирать достаточно большие простые числа и подходящие параметры группы.

Схема Шнорра – это асимметричная схема подписи, основанная на сложности вычисления дискретного логарифма. Криптостойкость схемы Шнорра зависит от сложности вычисления дискретного логарифма в использованной группе. При использовании достаточно больших простых чисел и безопасной группы, схема Шнорра считается криптостойкой.

DSA – это схема подписи, основанная на сложности вычисления дискретного логарифма в конечных полях. Криптостойкость DSA также зависит от сложности вычисления дискретного логарифма и выбранных параметров. Для обеспечения криптостойкости DSA необходимо выбирать достаточно большие простые числа.

1. Какие элементы составляют ключевую информацию алгоритмов реализации ЭЦП, перечисленных в вопросе 6?

RSA:

– Публичный ключ RSA, который состоит из пары чисел (n, e), где n - модуль, а e - открытая экспонента.

– Приватный ключ RSA, который состоит из пары чисел (n, d), где n - модуль, а d - закрытая экспонента.

Схема Эль-Гамаля:

– Параметры группы, которые включают простое число p - модуль, g - генератор группы, и вычисленное значение y.

– Приватный ключ, который представляет собой случайное число x, выбранное из определенного диапазона.

Схема Шнорра:

– Параметры группы, которые включают простое число p - модуль, q - порядок подгруппы, g - генератор подгруппы.

– Приватный ключ, который представляет собой случайное число x, выбранное из определенного диапазона.

DSA:

– Параметры группы, которые включают простое число p - модуль, q - порядок подгруппы, g - генератор подгруппы.

– Публичный ключ DSA, который представляет собой пару чисел (p, q, g, y), где p, q, g - параметры группы, а y - открытый ключ.

– Приватный ключ DSA, который представляет собой случайное число x, выбранное из определенного диапазона.

1. Дать сравнительные характеристики схемам ЭЦП, перечисленным в вопросе 6.

RSA:

Преимущества:

* Широко применяется и поддерживается множеством программных и аппаратных средств.
* Высокая скорость создания подписи и проверки подписи.

Недостатки:

* Более высокий уровень вычислительной сложности по сравнению с некоторыми другими алгоритмами.
* Требует большие значения ключей для обеспечения достаточного уровня безопасности.

Схема Эль-Гамаля:

Преимущества:

* Хорошая криптостойкость на основе вычисления дискретного логарифма.
* Возможность использовать алгоритм для обмена ключами.

Недостатки:

* Более медленная скорость создания подписи и проверки подписи по сравнению с RSA.
* Большой размер подписи.

Схема Шнорра:

Преимущества:

* Простота и эффективность в реализации.
* Хорошая криптостойкость на основе вычисления дискретного логарифма.

Недостатки:

* Размер подписи больше, чем у некоторых других алгоритмов.
* Требуется внимание к безопасности при генерации случайных чисел.

DSA:

Преимущества:

* Хорошая криптостойкость на основе вычисления дискретного логарифма.
* Относительно меньший размер подписи по сравнению с некоторыми другими алгоритмами.

Недостатки:

* Более медленная скорость создания подписи и проверки подписи по сравнению с RSA.
* Требуется выбор и генерация безопасных параметров группы.

1. Охарактеризовать особенности государственного стандарта ЭЦП в Республике Беларусь.

Государственный стандарт электронной цифровой подписи (ЭЦП) в Республике Беларусь регулируется законодательством и нормативными актами, включая следующие особенности:

* Обязательность использования государственного стандарта: В Беларуси существует обязательное требование использования государственного стандарта ЭЦП при организации электронного документооборота в государственных органах, организациях и предприятиях, а также при взаимодействии с государственными информационными системами.
* Утверждение государственного стандарта: В Беларуси государственный стандарт ЭЦП утверждается соответствующими государственными органами и организациями, которые определяют требования к алгоритмам, параметрам и форматам ЭЦП, а также процедуры проверки и аттестации систем и средств ЭЦП.
* Требования к ключевой информации: Государственный стандарт ЭЦП включает требования к генерации, использованию и хранению ключевой информации, включая форматы ключей, параметры алгоритмов и применение криптографических алгоритмов, соответствующих международным стандартам и рекомендациям.
* Аттестация систем и средств ЭЦП: Государственный стандарт предусматривает процедуры аттестации систем и средств ЭЦП, которые позволяют проверить соответствие используемых решений требованиям безопасности и функциональности, установленным в стандарте.
* Установление правового статуса: Государственный стандарт ЭЦП в Республике Беларусь имеет правовой статус и определяет юридическую силу электронных документов, подписанных с использованием соответствующих ключей и алгоритмов, в соответствии с законодательством Республики Беларусь.

**Вывод:** в ходе лабораторной работы были изучены алгоритмы генерации и верификации электронной цифровой подписи, а также приобретены практические навыки их реализации. Также была оценена скорость генерации и верификации ЭЦП.