МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»
Кафедра систем информационной безопасности

«ДОПУЩЕН К ЗАЩИТЕ»
Зав. кафедрой к.п.н., доцент Р. Ш. Бердибаев
_____ «_____» _____2019 г.
(подпись)

ДИПЛОМНЫЙ ПРОЕКТ

На тему: Проектирование устройства умножения по модулю на делительных устройствах с восстановлением остатков
Специальность: 5В100200 – «Системы информационной безопасности»
Выполнила Аскарова Виктория Группа СИБ-15-3
Научный руководитель Тынымбаев Сахыбай Тнейбаевич

Консультанты:
по экономической части:
к. э. н., профессор Ибрибаева Ж. Т.
(ученая степень, звание, Ф.И.О)
(подпись) «28» мая 2019 г.

по безопасности жизнедеятельности:
к.т.н. ст. преп. Бекбасаров Ш.И.
(ученая степень, звание, Ф.И.О)
(подпись) «22» мая 2019 г.

по применению вычислительной техники:
к.т.н. проф. Тынымбаев С.Т.
(ученая степень, звание, Ф.И.О)
(подпись) «28» мая 2019 г.

Нормоконтролер:
Ст. преподаватель Аскарова Н.Т.
(ученая степень, звание, Ф.И.О)
(подпись) «7» июня 2019 г.

Рецензент:
к.ф.-м.н., Мусирамиева Ш.Ш.
(ученая степень, звание, Ф.И.О)
(подпись) «____» _____2019 г.

Алматы 2019

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ КАЗАХСТАН
Некоммерческое акционерное общество
«АЛМАТИНСКИЙ УНИВЕРСИТЕТ ЭНЕРГЕТИКИ И СВЯЗИ»

Институт систем управления и информационных технологий

Кафедра систем информационной безопасности

Специальность 5В100200 – «Системы информационной безопасности»

ЗАДАНИЕ
на выполнение дипломного проекта

Студенту Аскаровой Виктории

Тема проекта: Проектирование устройства умножения по модулю на делительных устройствах с восстановлением остатков

Утверждена приказом по университету №124 от «26» 10 2018 г.

Срок сдачи законченного проекта «28» мая 2019 г.

Исходные данные к проекту (требуемые параметры результатов исследования (проектирования) и исходные данные объекта): проект подразумевает проектирование устройства умножения по модулю на делительных устройствах с восстановлением остатков, изучение методов приведения чисел по модулю при помощи аппаратной реализации устройства. Изучение существующих алгоритмах ассиметричного шифрования.

Перечень вопросов, подлежащих разработке в дипломном проекте, или краткое содержание дипломного проекта: дипломный проект включает в себя 5 глав, разделенных на подглавы, каждая из которых освещает определенную тематику.

В первой главе дипломного проекта представлена общая теоритическая информация о криптосистемах.

Во второй главе дипломного проекта представлены методы приведения чисел по модулю.

В третей главе подробно описывается разработка схемных решений быстродействующего устройства приведения чисел по модулю.

В четвертой главе приводится технико-экономическое обоснование проекта.

В пятой главе рассматриваются необходимые условия для комфортной разработки программного обеспечения.

Консультации по проекту с указанием относящихся к ним разделов проекта

Раздел	Консультант	Сроки	Подпись
Безопасность жизнедеят.	Бекбассаров Ш.Ш.	14.02-22.05.19	
Экономический раздел	Аренбаева Ж. Г.	04.03-28.05	
Вычислительной техники	Тынымбаев С.Т.	18.02-27.05.19	

График
подготовки дипломного проекта

Наименование разделов, перечень разрабатываемых вопросов	Сроки представления научному руководителю	Примечание
Содержание основ. принципов	04.03-08.03.2019	
Математические основы ассим. инф.	11.03-16.03.2019	
Дополнительные возм. аппарат. интерф.	29.03-13.04.2019	
Классификация и кратк. характ.	15.04-17.04.2019	
Способы привед. числ. полей	19.04-23.04.2019	
Оценка эфф. работ операторов	24.04-25.04.2019	
Деление с восстановлением остатка	27.04-03.05.2019	
Программирование схем упр. привед. числ.	04.05-14.05.2019	
Структур. схема контейнерной машины	14.05-17.05.2019	
Технико-экономич. обоснование	17.05-18.05.2019	
Безопасность жизнедеят.	19.05-20.05.2019	

Дата выдачи задания «22» октября 2018 г.

Заведующий кафедрой _____ (_____)
(Подпись) (Ф.И.О)

Научный руководитель проекта _____ (Тимофеев С.М.)
(Подпись) (Ф.И.О)

Задание принял к исполнению студент _____ (Аскарова Виктория)
(Подпись) (Ф.И.О)

АННОТАЦИЯ

В дипломном проекте были спроектированы схемные решения быстродействующих устройств приведения чисел по модулю, рассмотрены методы приведения чисел по модулю, аппаратная реализация и аппаратное ускорение выполнения шифрования.

Глава по безопасности жизнедеятельности характеризует благоприятные условия труда. В экономической части были приведены расчеты затрат на создание ПО и прибыль предприятия в случае внедрения предлагаемой модели.

АҢДАТПА

Дипломдық жұмыста модульдік сандарды үшін жоғары жылдамдықты құрылғыларға арналған тізбекті шешімдер әзірленді, сандарды өзгертуге, аппараттық қамтамасыз етуді және шифрлауды аппараттық жеделдету әдістерін қарады.

Өмір сүру қауіпсіздігі туралы тарау қолайлы жұмыс жағдайын сипаттайды. Экономикалық бөлімде ұсынылған модель енгізілген жағдайда, бағдарламалық қамтамасыз етуді жасау шығындары және кәсіпорынның пайдасы есептелді.

ANNOTATION

In the diploma project were designed circuit solutions for high-speed devices for modulating numbers, considered methods for modifying numbers, hardware implementation, and hardware acceleration of encryption.

The chapter on life safety characterizes favorable working conditions. In the economic part, calculations were made of the costs of creating software and the profit of the enterprise in the case of the introduction of the proposed model.

Содержание

Введение

Одним из самых распространенных методов защиты информации является шифрование. Оно основано на преображении текста, то есть информации, которую нужно защитить, в зашифрованное сообщение (шифротекст, криптограмму) при помощи криптографического алгоритма. На сегодняшний день существует множество криптосистем как с симметричным, так и с ассиметричным шифрованием.

Симметричные алгоритмы шифрования используют, как правило, один ключ для шифрования и дешифрования. Симметричные алгоритмы затрачивают намного меньше ресурсов, нежели ассиметричные, поэтому они хорошо подходят для шифрования большого объема данных, однако минусом является то, что отправитель должен располагать безопасным способом передачи закрытого ключа.

Ассиметричные алгоритмы шифрования, которые так же называются системами с открытым ключом, используют два ключа – закрытый и открытый.

Таким образом данные, зашифрованные одним ключом, возможно расшифровать только парным его ключом. Открытый ключ данной криптосистемы является публичным, то есть его предоставляют в широком доступе, а в тайне остается лишь закрытый ключ. Наиболее известными алгоритмами шифрования являются: Эль-Гамаля, Рабина, Диффи-Хелмана, Фита-Шамира, RSA и т.д.

Ассиметричное шифрование в основном применяется в разных протоколах данных, например: SSH, SSL/TLS, S/MIME для аутентификации, помимо это и в системах, требующих установки безопасного соединения в незащищенной сети. Так же ассиметричное шифрование используется в электронно-цифровой подписи (ЭЦП).

Алгоритм шифрования можно реализовывать аппаратным, программным и программно-аппаратным способами. Программный способ подразумевает собой создание программы на каком либо языке, на основе криптоалгоритма. При аппаратном шифровании, который реализован на основе вычислительного устройства. Соответственно последний это совмещенный способ шифрования.

Таким образом, тема дипломной работы является весьма актуальной в наше время.

Объектом исследования является быстродействующие устройство приведения чисел по модулю

Предметом исследования выступает устройство

Для достижения поставленной цели необходимо решить следующие задачи:

- изучить теоретические основы компонентов шифрования, их классификацию;
- рассчитать экономическую эффективность
- изучить роль вентиляции в здании;

– информационной базой данной дипломной работы является учебно-методологическая литература отечественных и зарубежных авторов, интернет-ресурсы.

1. Теоретические основы криптосистем

1.1 Криптографические алгоритмы, применяемые для обеспечения информационной безопасности.

Современная криптография делится на два вида - это симметричная и асимметричная. Симметричная применяется на потоковый шифр, блочный и составной. Асимметричная криптография более затратная по ресурсам, а в симметричной существует проблема эффективного распределения ключей. Современные системы безопасного обмена основаны на применении смешанной криптографии. В начале сеанса обмена стороны пересылают друг другу посредством асимметричной криптографии секретные сеансовые ключи, которые используются далее для симметричного шифрования пересылаемых данных. Система асимметричной криптографии позволяет распределять ключи в симметричных системах шифрования.

Криптография - это метод защиты информации и сообщений с использованием кодов, чтобы их могли прочитать и обработать только те, для кого предназначена информация.

В области компьютерных наук криптография относится к защищенным информационным и коммуникационным методам, полученным из математических понятий, и серии вычислений, основанных на правилах, называемых алгоритмами для преобразования сообщений способом, который трудно декодировать. Эти детерминированные алгоритмы используются для генерации криптографических ключей, цифровых подписей и проверок защиты конфиденциальности, работы в Интернете и конфиденциальных сообщений, таких как транзакции по кредитным картам и электронные письма.

Криптографические методы

Криптография тесно связана с дисциплинами криптологии и криптоанализа. Он включает в себя такие методы, как микроточки, слияние слов с изображениями и другие методы сокрытия информации в хранилище или во время передачи. Однако в современном компьютерно-ориентированном мире криптография обычно ассоциируется с шифрованием простого текста (простого текста, иногда называемого открытым текстом) в шифротекст (процесс, называемый шифрованием), а затем обратно (называемый дешифрованием). Люди, которые практикуют эту область, известны как криптографы.

Современная криптография решает следующие четыре задачи:

Конфиденциальность: информация не может быть понята тем, для кого она была непреднамеренной

Целостность: информация не может быть изменена во время хранения или передачи между отправителем и предполагаемым получателем без обнаружения изменений

Надежность: создатель / отправитель информации не может отрицать свои намерения в производстве или передаче информации в более поздние сроки

Аутентификация: отправитель и получатель могут взаимно подтвердить идентичность и происхождение / назначение информации

Процедуры и протоколы, которые соответствуют некоторым или всем вышеперечисленным критериям, называются криптосистемами. Предполагается, что криптосистемы относятся только к математическим процедурам и компьютерным программам; Тем не менее, они также включают в себя регулирование поведения человека, такое как выбор трудно угадываемых паролей, постепенный отказ от неиспользуемых систем и отказ обсуждать конфиденциальные процедуры с посторонними.

Криптографические алгоритмы

Криптосистемы используют различные методы, известные как криптографические алгоритмы или шифры, для шифрования и дешифрования сообщений для защиты связи между компьютерными системами, устройствами, такими как смартфоны, и приложениями. Набор шифров использует один алгоритм для шифрования, другой алгоритм для аутентификации сообщений и другой для обмена ключами. Этот процесс, встроенный в протоколы и написанный в программном обеспечении, работающем в операционных системах и сетевых компьютерных системах, включает генерацию открытых и закрытых ключей для шифрования / дешифрования данных, цифровую подпись и проверку подлинности сообщений и обмена ключами.

В последнее время криптография стала полем битвы некоторых из лучших в мире математиков и программистов. Способность надежно хранить и передавать конфиденциальную информацию оказалась решающим фактором в войне и успехе в бизнесе.

Поскольку правительства не хотят, чтобы конкретные организации в их странах и за их пределами имели доступ к методам получения и отправки скрытой информации, которая может угрожать их национальным интересам, криптография во многих странах подвергается различным ограничениям, включая ограничения на ее использование и экспорт программного обеспечения. Для широкой публики распространяются математические концепции развития криптосистем. Тем не менее, Интернет позволил распространить мощные программы и, что более важно, основные криптографические методы, так что сегодня многие из самых передовых криптосистем и идей находятся в открытом доступе.

Криптографические проблемы

Злоумышленники могут обойти криптографию, взломать компьютеры, отвечающие за шифрование и дешифрование данных, и использовать слабые реализации, такие как: В. Стандартный ключ. Однако криптография затрудняет доступ злоумышленников к сообщениям и данным, которые защищены алгоритмами шифрования.

Растущая обеспокоенность вычислительной способностью квантовых компьютеров нарушать современные стандарты криптографического шифрования побудила Национальный институт стандартов и технологий в 2016 году обратиться к математическому и научному сообществу с просьбой ввести новые стандарты криптографии с открытым ключом. В отличие от современных компьютерных систем, квантовые вычисления используют квантовые биты (кубиты), которые могут представлять как 0, так и 1, и, таким образом, выполняют два одновременных вычисления. Хотя большой квантовый компьютер может не быть построен в следующем десятилетии, существующая инфраструктура требует стандартизации хорошо известных и понятных алгоритмов, которые согласно NIST предлагают безопасный подход. Крайний срок подачи заявок - ноябрь 2017 года, а анализ предложений, как ожидается, займет от трех до пяти лет.

Свойство конфиденциальности информации ее доступность строго ограниченному кругу лиц, определение которых находится в компетенции ее владельца. В том случае, если доступ к данным получает неуполномоченный субъект, можно констатировать утрату конфиденциальности. [40, с. 24]

Важно отметить, что для определенной информации обеспечение ее конфиденциальности – ключевое требование. Например, информация, относящаяся к государственной тайне, данные научных исследований и инновационных разработок, информация, связанная с хранением и обработ-кой персональных данных. Последняя особенно важна для таких учрежде-ний как государственные организации, финансово-кредитные компании, медицинские лаборатории и клиники. [17, с. 45]

Целостность как следующее свойство информации рационально определить, как способность сохраняться в неискаженном виде. Нарушение данного свойства возможно в случае неправомерных, не предусмотренных создателем информации, действий, связанных с внесением каких-либо изменений. Обеспечение данного свойства информации критически важно для объектов сложного управления: аппаратно-программных платформ координации воздушного движения, энергоснабжения, финансовых платформ.

Доступность информации это способность предоставлять регламентированный доступ тем субъектам, которые обладают определенными правами и полномочиями. Блокирование и уничтожение – основные методы нарушения доступности информации. [30, с. 59]

С точки зрения прикладной значимости, доступность – важное свойство информационных систем, обслуживающих различные категории населения и бизнеса. Например, системы бронирования средств размещения, билетов на различные виды транспорта, обновление программного обеспечения. Нарушение доступность подобной информации называют отказом в обслуживании, что негативно сказывается на репутации компании и лояльности к ней клиентов.

Физические средства защиты информации применяются для организации охраны технической инфраструктуры сети. Достижение данной

цели возможно с применением инженерных устройств, приспособлений и сооружений, которые препятствуют проникновению нарушителей в технические составляющие сети. Например, с помощью средств охранной сигнализации, биометрических замков может обеспечивать безопасность серверного центра организации. [36, с. 211]

Аппаратные средства защиты информации включают электронные, электромеханические устройства, используемые для защиты внутренних ресурсов компьютерной сети: например, терминалов доступа, линий связи, процессоров серверов, периферийного оборудования. Их преимущество состоит в высокой степени защиты, исключение вмешательства в их работу из сети, высокий уровень производительности, что особенно важно в процессе реализации криптографических методов. Несмотря на большой спектр преимуществ, данные средства защиты информации в сетях имеют важный недостаток – высокая стоимость – что критично для малых предприятий в условиях экономического кризиса. [19, с. 58]

Программные средства защиты информации в сетях объединяют приложения и программные комплексы, реализующие те или иные методы обеспечения безопасности данных. Среди преимуществ данных средств рационально выделить их большой ассортимент на рынке, невысокую стоимость, простоту применения, универсальной, возможность адаптации и масштабирования, гибкость. Недостатками программных средств считается их доступность для хакеров, что особенно касается лидеров данного рынка ПО. [20, с. 15]

Реализация программных средств защиты информации в сетях возможна в сетевых операционных системах и специализированных серверных приложениях.

Симбиозом программных и аппаратных средств защиты информа-ции в сетях являются аппаратно-программные средства. Их основное преимущество – идеальный баланс между высокой производительной аппаратной части и гибкостью программных приложений. Среди данных средств защиты информации в сетях лидером являются маршрутизаторы фирмы Cisco. [10, с. 67]

Организационные средства защиты информации включают определения предписания, инструкции и распоряжения руководство предприя-тия, регламентирующие функционирование и использование ресурсов се-ти. Важно отметить, что данные средства предписывают определенные правила поведения персонала, их возможные случаи взаимодействия с ре-сурсами сети в той мере, чтобы обеспечить наибольший уровень защиты информации и максимально снизить вероятность реализации угроз. [14, с. 38]

Организационные средства защиты информации в сетях включают в себя следующие мероприятия:

– направленные на оптимальный отбор и подготовку кадров относительно использования ресурсов сети;

– применяемые при проектировании, модернизации и обслуживании сети;

– составляющие основу политики безопасности;

– регламентирующие учет, анализ и мониторинг инцидентов нарушения безопасности информации в сетях;

– применяемые при выборе и замене аппаратно-программного обеспечения сетей и т.п. [3, с. 20-22]

Недостатком организационных средств защиты информации в сетях является нерациональной их применения без поддержки физических, программных и аппаратных средств. Некоторые небольшие компании отказываются от данных средств защиты информации в сетях из-за возникнове-ния формальностей и рутинной работы, связанной с созданием, контролем реализации данных мероприятий. [12, с. 48]

Законодательные средства защиты информации в сетях - это совокупность нормативно-правовых документов, регламентирующих правиль-ное использование информации, которая является государственной тай-ной, связана с обработкой персональных данных и т.п. Важно отметить, что соблюдение требований законодательства обеспечивается с помощью установления ответственности за их нарушения: уголовной или административной.

Морально-этические средства защиты информации в сетях включа-ют определенные нормы поведения, нарушение которых ведет к снижению авторитетности и репутации члена социума или предприятия. Данные средства могут быть общепринятыми, например, честность, патриотизм, так и оформленными в кодекс или свод правил. [23, с. 26]

Таким образом, описанные выше средства защиты информации в сетях можно разделить на две группы:

1) формальные, которые выполняют функции обеспечения безопасности информации по определенной процедуре без участия субъектов.

2) неформальные, которые обусловлены определенной деятельностью пользователей либо регламентируют ее.

Рациональная и эффективная система защиты информации в сетях возможна только в случае использования совокупности данных средств, выбранных относительно определенной ситуации организации, отрасли, рынка, возможных угроз и ценности защищаемых данных. [9, с. 41]

Таким образом, рационально организованная система защиты информации в сетях должна обладать следующими свойствами:

– стоимость выбранных средств обеспечения безопасности должна быть соизмерима с размерами возможного ущерба;

– субъект компьютерной сети должен иметь минимальным набором прав, необходимый для выполнения только функциональных задач;

– эффективность системы защиты информации прямо пропорционально удобству работы пользователя с ней;

– система защиты информации должна предусматривать возможность аварийных ситуаций и отказов в обслуживании;

– обслуживающий персонал системы защиты информации в сети должны обладать всеми необходимыми компетенциями и пониманием сущности ее функционирования;

– защищаемой должна являться вся информация, циркулирующая в сети, вне зависимости от ее типа и значимости;

– разработчики системы защиты информации в сети, не должны быть в числе тех, кого эта система будет контролировать;

– система защиты должна обладать средством проверки корректности ее работы;

– система защиты информации в сети должна быть рассчитаны на любые действия пользователей;

– контроль над системой защиты должен иметь человек, принимающий решения в организации. [44, с. 122-128]

1.2 Математические основы асимметричного шифрования.

Основная идея асимметричного шифрования заключается в одновременном существовании двух ключей для обмена информацией - открытого, известного каждому и частного, известного только получателю информации. Как и должно быть, оба ключа (закрытый и открытый) создаются одновременно с использованием математических вычислений, и между ними существует четкая связь. Основная задача разработчика асимметричного алгоритма состоит в том, что с использованием открытого ключа невозможно (очень долго) получить секретный ключ шифрования. Для этой цели асимметричные алгоритмы основаны на сложных задачах вычисления факторизации, дискретной логарифмизации, проекции точек на эллиптической кривой и т. Д. Все эти задачи объединены тем, что они используют операцию, чтобы вывести остаток из целочисленного деления.

Для шифрования данных сегодня используются 3 наиболее часто аналогичные методы шифрования: аппаратное, программное и аппаратное обеспечение, а также программное обеспечение. Их основное отличие заключается не только в том, как они реализуют шифрование и надежность защиты данных, но и в затратах, которые зачастую являются решающим моментом для пользователей. Самые дешевые устройства шифрования - это программное обеспечение, а затем программное и аппаратное обеспечение, самое дорогое устройство. Несмотря на то, что стоимость аппаратных кодеров важнее программного обеспечения, разница в стоимости несопоставима со значительным повышением безопасности данных.

1.3 Достоинства аппаратного шифрования

Большое количество инструментов шифрования данных создаются как специализированные физические устройства. Программные кодировщики

обычно дешевле аппаратных средств и в некоторых случаях могут ускорить обработку информации. Список преимуществ аппаратных кодеров:

1) Аппаратный генератор случайных чисел генерирует истинные случайные числа для формирования надежных ключей шифрования и цифровой подписи.

2) аппаратная реализация криптоалгоритма обеспечивает его целостность;

3) Ключи шифруются и хранятся в самом кодере, а не в оперативной памяти компьютера.

4) Ключи загружаются электронными клавишами с сенсорной памятью (i-button) и смарт-картами непосредственно в криптографическое устройство, а не через системную шину компьютера и память ОЗУ, что исключает перехват ключей.

5) Используя аппаратные кодировщики, вы можете внедрить системы, позволяющие различать доступ к компьютеру и защищать информацию от несанкционированного доступа.

6) использование специализированного процессора для выполнения всех расчетов освобождает центральный процессор компьютера; Вы также можете установить несколько аппаратных кодеров на одном компьютере, что еще больше увеличит скорость обработки информации (это преимущество присуще кодерам шины PCI).

7) Использование парафазной шины при создании криптографического процессора исключает опасность считывания ключевой информации о вибрациях электромагнитного излучения, вызванных шифрованием данных в заземляющих цепях устройства.

8) Шифрование данных быстрее программного и аппаратного шифрования

Проблем с установкой на компьютер специальных устройств шифрования меньше, чем с добавлением функций шифрования данных в системное программное обеспечение. Шифрование в лучшем случае должно быть таким, чтобы пользователь не заметил. Чтобы сделать это с помощью программного обеспечения, они должны быть достаточно глубоко спрятаны в операционной системе. Очень трудно легко выполнить эту операцию с отлаженной операционной системой. Любой непрофессионал может подключить устройство шифрования к ПК или модему.

Типы аппаратных устройств шифрования

Современный рынок предлагает три типа аппаратного шифрования информации:

1) Блоки шифрования в каналах связи

2) модули автаркического шифрования (они самостоятельно выполняют всю работу с ключами)

3) Шифрование карт расширения для установки на ПК

Почти все устройства первых двух типов являются узкоспециализированными. Поэтому перед принятием окончательного

решения о покупке необходимо внимательно изучить ограничения, которые эти устройства накладывают на свои устройства, прикладное программное обеспечение и операционные системы во время установки. В противном случае вы можете потратить деньги зря, не достигнув желаемой цели. Однако есть компании, которые продают устройства связи с предустановленными аппаратными устройствами шифрования, что иногда облегчает выбор.

Платы расширения для ПК являются более универсальным средством аппаратного шифрования, и их обычно очень легко настроить для шифрования всей информации, записанной на жесткий диск или отправленной в порты и жесткие диски. Обычно в платах расширения аппаратного шифрования отсутствует защита от электромагнитного излучения, поскольку бесполезно защищать эти карты, если только весь компьютер не защищен аналогичным образом.

1.4 Дополнительные возможности аппаратных шифраторов

Использование всей платы расширения для аппаратного шифрования само по себе слишком расточительно. В дополнение к функциям шифрования производители пытаются добавить различные дополнительные функции на свои устройства, например:

Генератор случайных чисел. Это необходимо в основном для генерации криптографических ключей. Кроме того, большое количество алгоритмов шифрования применяют их для других целей. Например, алгоритм электронной подписи ГОСТ Р 34.10 - 2001: При расчете подписи каждый раз используется новое случайное число.

Надежная загрузка. Контроль ввода на компьютер. Каждый раз, когда пользователь включает персональный компьютер, устройство будет требовать от него ввода личной информации (например, вставить дискету с ключами). Только если устройство распознает предоставленные ключи и считает их «своими», загрузка продолжится. В противном случае пользователь должен будет разобрать компьютер и удалить оттуда плату кодера, чтобы включить компьютер (однако, как вы знаете, информация на жестком диске также может быть зашифрована).

Контроль целостности файлов операционной системы. Злоумышленник не сможет ничего изменить в ваше отсутствие в ваше отсутствие. Кодировщик сохраняет в своей памяти список всех важных файлов с предварительно рассчитанными контрольными суммами для каждого (или значения хеш-функции), и компьютер будет заблокирован, если при следующей загрузке не совпадет контрольная сумма хотя бы одного из файлов.

Устройство криптографической защиты данных (LADD) является платой расширения со всеми вышеупомянутыми возможностями. Аппаратное устройство шифрования, которое контролирует доступ к ПК и проверяет целостность всех файлов операционной системы, также называется «электронная блокировка». Понятно, что аналогия не совсем полная, обычные замки намного уступают этим умным устройствам. Хотя очевидно, что для

последнего требуется программное обеспечение, необходима утилита, которая генерирует ключи для пользователей и сохраняет их список для идентификации «их / других». Вам также понадобится программа для выбора важных файлов и расчета их контрольных сумм. Доступ к этим приложениям обычно доступен только администратору безопасности. Он должен заранее настроить все устройства для пользователей и понять их причины в случае возникновения проблем.

Симметричное шифрование

Алгоритмы с симметричным ключом иногда называют алгоритмами с секретным ключом. Это связано с тем, что в этих типах алгоритмов обычно используется один ключ, который хранится в секрете системами, участвующими в процессах шифрования и дешифрования. Этот единственный ключ используется как для шифрования, так и для дешифрования.

Алгоритмы с симметричным ключом имеют тенденцию быть очень безопасными. В целом они считаются более безопасными, чем алгоритмы с асимметричным ключом. Существует несколько алгоритмов симметричного ключа, которые считаются практически неразрушимыми. Алгоритмы с симметричным ключом также очень быстрые. Вот почему они часто используются в ситуациях, когда существует много данных, которые необходимо зашифровать.

В алгоритмах симметричного ключа ключ распределяется между двумя системами. Это может представлять проблему. Вы должны найти способ получить ключ ко всем системам, которые должны будут шифровать или дешифровать данные, используя алгоритм симметричного ключа. Распределение ключа по всем системам вручную может быть довольно громоздкой задачей. Иногда это можно сделать только путем копирования ключа из центрального расположения. Вы можете себе представить, как это может быть неприятно. В системах Windows у вас есть возможность использовать групповую политику или какой-либо сценарий для копирования ключа в необходимые системы. Это помогает, но администратор по-прежнему несет ответственность за правильное функционирование групповой политики или сценария.

Алгоритмы симметричного ключа

Существуют сотни различных алгоритмов симметричного ключа. У каждого есть свои сильные и слабые стороны. Некоторые из наиболее распространенных примеров - DES, 3DES, AES, IDEA, RC4 и RC5.

DES: Это стандарт шифрования данных. DES был первоначально разработан в 1976 году. Он был одним из наиболее широко используемых алгоритмов шифрования. Отчасти это связано с тем, что он был принят в качестве государственного стандарта для шифрования. Сам алгоритм DES очень силен. Слабость заключается в том, что в оригинальном стандарте DES используется 56-битный ключ шифрования. По сути, вы можете использовать компьютер для запуска всех битовых комбинаций клавиши (1 и 0), пока не нажмете правую клавишу. Назад, когда DES был первоначально разработан,

это заняло бы сотни лет. В наши дни компьютеры намного, намного быстрее. На самом деле, в настоящее время для прохождения всех комбинаций может потребоваться всего один день или около того. Это основная причина, почему DES больше не используется широко.

3DES: это наиболее известный как Triple DES. 3DES получил свое имя, потому что он применяет алгоритм DES три раза к каждому блоку данных. 3DES обогнал своего предшественника, DES, и в настоящее время считается наиболее широко используемым стандартом для безопасного шифрования. Сам алгоритм такой же сильный, как DES, но у вас также есть преимущество, заключающееся в возможности использовать более длинные ключи. Ключ должен быть указан для каждой итерации шифрования 3DES. У вас есть возможность использовать один и тот же ключ для каждой, один и тот же для двух итераций или другой ключ для каждой из итераций. Наиболее безопасная реализация - использовать разные ключи для каждой итерации. Если вы используете один и тот же ключ для всех трех итераций, сила ключа будет равна 56 битам. Это в основном так же, как DES. Если вы используете один и тот же ключ для двух итераций и другой ключ для третьей, то сила ключа считается равной 112 битам. Если вы используете разные ключи для всех трех итераций, то степень шифрования считается равной 168 битам. Долгое время алгоритм 3DES был основным алгоритмом, используемым в реализациях Windows FIPS 140 для жалоб. Когда вы настраивали групповую политику Windows или реестр, который принудительно использовал алгоритмы, совместимые с FIPS 140, вы в основном заставляли использовать 3DES для шифрования. Теперь системы Windows предлагают использование AES, который также является алгоритмом, совместимым с FIPS 140.

AES: это расширенный стандарт шифрования. Его также иногда называют алгоритмом Рейндаэля. Это связано с тем, что AES фактически происходит из алгоритма Rijndael. В правительстве был проведен процесс оценки, чтобы определить, какой алгоритм будет использоваться в качестве стандарта AES, и в качестве победителя был выбран алгоритм Rijndael. Стандарт AES фактически включает в себя три разных шифра: AES-128, AES-192 и AES-256. Числа представляют длину ключа шифрования. AES очень быстрый и очень безопасный. Из-за этого его глобальное внедрение было очень быстрым.

IDEA_: это международный алгоритм шифрования данных. Изначально IDEA должна была заменить стандарт DES. IDEA использует 128-битный ключ шифрования. Есть две основные причины, по которым IDEA не так широко используется, как планировалось. Во-первых, это тот факт, что IDEA подвержена ряду слабых клавиш. Вторая причина заключается в том, что в настоящее время существуют более быстрые алгоритмы, обеспечивающие такой же уровень безопасности.

RC4: Это четвертая версия Rivest Cipher. RC4 использует ключ шифрования переменной длины. Этот ключ может варьироваться от 40 до 256 бит. Это чаще всего используется с 128-битным ключом. Алгоритм RC4 очень

прост и легко реализуем. Проблема заключается в том, что, если реализовано неправильно, это может привести к слабым криптографическим системам. Это одна из главных причин, по которой RC4 постепенно выводится из употребления. RC4 был одним из наиболее широко используемых алгоритмов шифрования. Он используется в WEP и WPA в беспроводных сетях. Он также использовался в протоколе Secure Sockets Layer (SSL) и на транспортном уровне (TLS) с протоколом передачи гипертекста по протоколу SSL (HTTPS). RC4 также используется с защищенной оболочкой, Kerberos и протоколом удаленного рабочего стола.

RC5: Это пятая версия Rivest Cipher. RC5 использует ключи шифрования переменной длины. Они могут варьироваться до 2040 бит. Рекомендуемый размер ключа составляет 128 бит. В какой-то момент RSA, которому принадлежит патент на RC5, был настолько уверен в своей безопасности, что у него была система вознаграждений, чтобы вознаграждать любого, кто мог взломать предметы, зашифрованные с помощью алгоритма. На рисунке 1.1 приведены длина ключа и размер блока для этих алгоритмов.

	Key Length	Block Size
DES	56 bits	64 bits
3DES	56, 112, or 168 bits	64 bits
AES	128, 192, or 256 bits	128 bits
IDEA	128 bits	64 bits
RC4	40 to 256 bits	Stream cipher
RC5	0 to 2040 bits (128 recommended)	32, 64, or 128 bits (64 recommended)

Рисунок 1.1 – Длина ключа различных алгоритмов

Криптография с открытым ключом

Алгоритмы симметричного ключа довольно эффективны, но распределение ключей затруднительно для конечных устройств IoT. Распределение ключей требует безопасного соединения между сервером распространения ключей и узлами IoT. PKC и асимметричная криптография являются двумя эффективными способами обеспечения конфиденциальности и аутентификации. В отличие от симметричной криптографии, в основе PKC лежит математически сложная задача, которая решается, тогда как в данном контексте под сложным понимается сложность вычислений. Шифрование с открытым ключом основано на функциях «люка», которые легко вычислить, но трудно перевернуть без дополнительной информации. RSA - это широко используемый алгоритм с открытым ключом, в котором трудной задачей является поиск основных факторов составного числа. В криптосистеме PKC, как правило, в виде пары ключей, открытого ключа и закрытого ключа, открытый ключ становится доступным для открытого, а закрытый ключ

хранится в безопасном месте. Открытый ключ обычно используется двумя способами.

1 Шифрование с открытым ключом, при котором можно зашифровать сообщение открытым ключом объекта, причем только объект с соответствующим закрытым ключом может расшифровать зашифрованный текст.

2 Цифровые подписи, в которых зашифрованный текст, созданный с помощью закрытого ключа, может быть расшифрован любым, кто имеет открытый ключ. Эта проверка подтверждает, что отправитель имел доступ к закрытому ключу и, следовательно, вероятно, был лицом, связанным с открытым ключом.

В системе PKC пары открытого / секретного ключей могут быть легко созданы для шифрования и дешифрования. Сила безопасности в системе PKC заключается в том, насколько сложно определить правильно сгенерированный закрытый ключ из его открытого ключа. В этом случае длина закрытого ключа важна для предотвращения атак методом перебора.

RSA - это одна из первых практических криптосистем с открытым ключом, основанная на практической сложности факторизации произведения двух больших простых чисел. Если открытый ключ достаточно велик, то только тот, кто знает простые числа, может реально декодировать сообщение. RSA является относительно медленным алгоритмом шифрования, однако он обычно используется для передачи зашифрованных общих ключей для криптографии с симметричным ключом. Поскольку шифрование RSA является дорогостоящей операцией, в IoT оно скорее используется в сочетании с симметричной криптографией. Общий симметричный ключ шифруется с помощью RSA; Безопасность шифрования в целом зависит от длины ключа. Для RSA требуется длина ключа 1024 бита (128 байтов), чтобы иметь эквивалентный уровень безопасности симметричного криптографического ключа с длиной ключа 128 бит (16 байтов). Большой размер ключа RSA приведет к дорогостоящим вычислительным затратам.

ECC является альтернативой обычному PKC из-за устойчивости к мощным атакам по исчислению индекса. ECC обеспечивает эффективную реализацию из-за значительно меньшего размера битов операндов в среде с ограниченными ресурсами. ECC - это еще один подход криптографии с открытым ключом, который работает на основе эллиптических кривых над конечными полями. Меньший размер ключа ECC равен 256, как показано на рисунке 1.2. Он более эффективен, чем RSA, и больше подходит для устройств с ограниченными ресурсами в IoT. Основной идеей ECC является общее предположение о том, что задача дискретного логарифма эллиптической кривой неосуществима или, по крайней мере, не разрешима в течение разумного времени.

Symmetric Key	RSA Key	Elliptic Curve Key
80	1024	160
112	2048	224
128	**3072**	**256**
192	7680	384
256	15,360	521

Рисунок 1.2 – Сравнение длины ключей

Алгоритмы с открытым ключом, также известные как алгоритмы асимметричного ключа, используются (главным образом) для решения двух задач, которые не могут быть реализованы алгоритмами симметричного ключа: распределение ключей и неотказанность. Первый помогает решить проблемы конфиденциальности, а второй помогает решить проблемы подлинности.

Алгоритмы с открытым ключом достигают этих целей, работая асимметрично; то есть ключ делится на две соответствующие части: открытый ключ и закрытый ключ. Открытый ключ назван так, что его можно безопасно разглашать всем, кто его запрашивает. Открытый ключ позволяет людям шифровать сообщения и проверять подписи. Закрытый ключ назван так, поскольку он должен оставаться закрытым и не может быть выдан. Закрытый ключ обычно принадлежит одному человеку или устройству в большинстве случаев, но технически может быть разделен между доверенным набором сторон. Закрытый ключ позволяет расшифровывать сообщения и генерировать подписи.

Первым публично раскрытым алгоритмом открытого ключа был обмен ключами Диффи-Хеллмана, который позволял, по крайней мере на начальном этапе, только для распределения ключей между известными сторонами. ElGamal расширила его до полной схемы шифрования и подписи с открытым ключом и, как мы вскоре увидим, используется для шифрования ECC. Вскоре после публикации Diffie-Hellman был публично представлен другой алгоритм, известный как RSA (Rivest Shamir Adleman). RSA допускает как шифрование, так и подписи, при этом используя половину полосы пропускания как ElGamal. Впоследствии RSA стал стандартизирован в различных формах.

Позже, в 1980-х годах, эллиптические кривые были предложены в качестве абелевой группы, над которой можно было выполнять шифрование ElGamal и DSA (вариант ElGamal), и в течение 1990-х и 2000-х годов были предложены различные алгоритмы, которые делают криптографию эллиптических кривых привлекательной альтернативой RSA. и Эль-Гамаль.

Для целей этого текста мы обсудим стандарт RSCS и криптографию ECC стандарта PKCS # 1. Они представляют два из трех стандартных

алгоритмов, определенных NIST для криптографии с открытым ключом, и в целом представляют требования коммерческого сектора.

1.5 Асимметричные алгоритмы шифрования

Асимметричное шифрование также известно как криптография с открытым ключом, который является относительно новым методом по сравнению с симметричным шифрованием. Асимметричное шифрование использует два ключа для шифрования простого текста. Секретные ключи обмениваются через Интернет или большую сеть. Это гарантирует, что злоумышленники не будут злоупотреблять ключами. Важно отметить, что любой пользователь с секретным ключом может расшифровать сообщение, и поэтому асимметричное шифрование использует два связанных ключа для повышения безопасности. Открытый ключ доступен всем, кто захочет отправить вам сообщение. Второй закрытый ключ хранится в секрете, чтобы вы могли только знать.

Сообщение, зашифрованное с использованием открытого ключа, может быть дешифровано только с использованием личного ключа, в то время как сообщение, зашифрованное с использованием личного ключа, может быть дешифровано с использованием открытого ключа. Безопасность открытого ключа не требуется, потому что он общедоступен и может быть передан через Интернет. Асимметричный ключ обладает гораздо большей силой в обеспечении безопасности информации, передаваемой во время связи.

Асимметричное шифрование в основном используется в повседневных каналах связи, особенно через Интернет. Популярный алгоритм шифрования асимметричного ключа включает в себя методы EIGamal, RSA, DSA, Elliptic Curve, PKCS.

Разница между симметричным и асимметричным шифрованием

Симметричное шифрование использует один ключ, который должен быть общим для людей, которым необходимо получить сообщение, в то время как асимметричное шифрование использует пару открытых ключей и секретный ключ для шифрования и дешифрования сообщений при передаче.

Симметричное шифрование является старой техникой, в то время как асимметричное шифрование является относительно новым.

Асимметричное шифрование было введено, чтобы дополнить внутреннюю проблему необходимости совместного использования ключа в симметричной модели шифрования, устраняя необходимость совместного использования ключа с помощью пары открытых и закрытых ключей.

Асимметричное шифрование занимает относительно больше времени, чем симметричное шифрование.

Электронная цифровая подпись

При обмене информацией между сторонами, которые не доверяют или заинтересованы в совершении действий, противоречащих друг другу (банк и клиент, бизнес и покупатель), должны использоваться методы асимметричного шифрования, а также ЭЦП. метод.

Необходимо не только конфиденциальность, но и согласие на сообщение (невозможность изменить сообщение или что-то изменить в нем), а также обеспечить авторство. Не веря, необходимо исключить возможность отказа разработчика новостей, отправив подписанное сообщение.

С помощью электронной подписи документа вы можете определить его подлинность. Криптографические средства также обеспечивают защиту от следующих злонамеренных действий:

1) Отказ - Абонент А заявляет, что он не отправил сообщение В, даже если он действительно отправил его;

2) Модификация - подписчик В изменяет документ и утверждает, что этот документ (измененный) был получен подписчиком А;

3) Замена - Участник В формирует документ (новый) и заявляет, что он получил его от Участника А;

4) Активный перехват - злоумышленник (подключенный к сети) перехватывает и изменяет документы (файлы).

5) «Маскарад» - партия Б отправляет документ на имя партии А;

6) Повтор - подписчик В повторяет ранее переданный документ, который подписчик А отправил абоненту В.

Все вышеперечисленные виды вредных действий наносят большой урон. Кроме того, вероятность злонамеренных действий подрывает доверие к компьютерным технологиям. Проблема аутентификации потенциально может быть решена на основе криптографического процесса выравнивания для разработки специальных алгоритмов и программ.

При выборе метода и технологии аутентификации вы должны обеспечить надежную защиту от всех перечисленных выше вредоносных действий (угроз). Однако в контексте обычного (одноключевого) секретного письма нелегко защитить от всех этих типов угроз из-за возможности злонамеренных действий одной из сторон с использованием секретного ключа.

Никто не может запретить подписчику, например, создать документ, зашифровать его в существующем ключе, который является совокупным для покупателя и банка, а затем заявить, что он получил документ от законного отправителя.

Внедрение систем, основанных на секретности двух ключей, считается эффективным. В этом случае каждая отправляющая сторона содержит личный закрытый источник подписи, и все участники имеют несекретные раскрытые ключи отправляющей стороны.

Эти раскрытые ключи могут быть интерпретированы как набор тестовых коэффициентов, которые позволяют осудить подлинность подписи отправителя, но не могут быть обновлены в обновленном секретном источнике. Отправляющий участник несет полную ответственность за личный секретный источник. Никто, не считающий его, не имеет возможности сделать настоящую подпись. Секретный источник отправляющей стороны может

рассматриваться как собственный закрытый ключ, и владелец должен каким-то образом ограничить доступ посторонних лиц.

Чтобы воплотить идею открытой энциклопедии в жизнь, необходимо найти конкретные и конструктивные ответы на следующие вопросы:

1) как «замесить» индивидуальный ключ пользователя с содержимым документа, чтобы он стал неразделимым?

2) как проверить подлинность содержимого подписываемого документа и индивидуального ключа, не зная заранее ни того, ни другого?

3) как обеспечить, чтобы автор повторно использовал один и тот же индивидуальный ключ для цифровой подписи большого количества электронных документов?

4) как гарантировать надежность индивидуального ключа пользователя для любого количества электронных документов, подписанных с ним?

5) Как гарантировать подлинность проверки цифровой подписи и содержания электронного документа?

6) Как обеспечить юридическую полноту электронного документа с цифровыми подписями, который существует без дубликата или другой замены?

Потребовалось около 20 лет, чтобы ответить на все эти вопросы с момента, когда эта идея впервые была сформулирована в 1976 году в статье Уитфилда Диффи и Мартина Хеллмана. Существует полный арсенал технических средств для авторизации электронных документов, называемых цифровыми подписями.

Современные принципы построения системы цифровой подписи просты и элегантны:

1) методы расчета и проверки цифровых подписей всех систем одинаковы и основаны на широко известных математических задачах;

2) известны способы вычисления ключей для цифровых подписей и цифровых ключей для цифровых подписей;

3) индивидуальные ключи для генерации цифровых подписей выбираются пользователями по случайному закону из большого набора всех возможных ключей;

4) с помощью специального алгоритма цифровой подписи его стойкость может быть оценена с использованием любой «закрытой» информации, основанной на известных математических результатах и разумных предположениях о вычислительной мощности потенциального взломщика. Средства криптографической защиты обеспечивают достоверность и достоверность информации, за исключением решения проблемы сохранения ее конфиденциальности. Эти функции выполняются с использованием технологии цифровой подписи. Схема работы цифровой подписи изображена на рисунке 1.3.

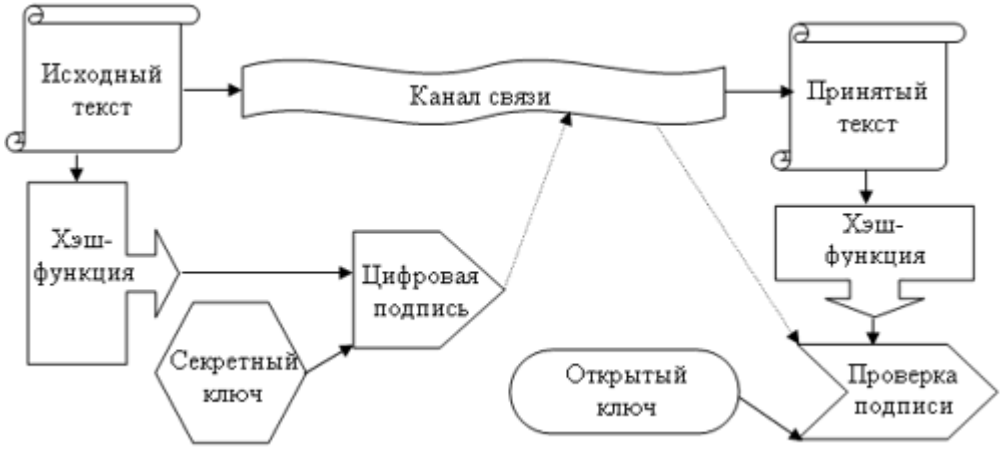

Рисунок 1.3 – Схема работы ЭЦП

На вход алгоритма поступает файл, необязательно текстовый, основное требование, предъявляемое к входным параметрам ЭЦП, – фиксированная длина, для этого используется хэш-функция.

1.6 Классификация криптоалгоритмов

Шифрование делится на два типа: симметричное и асимметричное. Короче говоря, ключ симметрично использует 2 ключа асимметрично. Симметричные криптосистемы делятся на два типа:

1) Системы блочного шифрования, суть в том, что информация делится на одинаково длинные блоки, на следующем шаге каждый блок шифруется отдельно ключом и, наконец, весь блок добавляется в шифр.

2) Потоковые шифры, в которых информация гамма преобразуется в биты. Потоковая криптосистема использует PRNG. PRNG выводит конкретную числовую последовательность. Последний накладывает зашифрованную информацию с помощью операции XOR. Операция XOR - это прежде всего строго дизъюнкция. Особенностью симметричного шифрования является скорость и простота реализации.

В асимметричном шифровании используются 2 ключа. Когда-то источник считается закрытым и известен только получателю. Используется для декодирования. Второй ключ является открытым. Он может быть общедоступным в сети и доступен по адресу пользователя. Используется для шифрования. Понятно, что источник расшифровки не может быть определен ключом шифрования. Наиболее популярным асимметричным методом является RSA (Raivest, Shamir, Adleman), основанный на операциях с большими (например, 100-значными) простыми числами и их произведениями.

1.7 Схема шифрования Эль Гамаля

«Схема Эль-Гамаля, предложенная в 1985 году, может использоваться как для шифрования, так и для цифровых подписей. Безопасность схемы Эль-

Гамаля обусловлена сложностью вычисления дискретных логарифмов в конечном поле.»

«Для того чтобы генерировать пару ключей (открытый ключ – секретный ключ), сначала выбирают некоторое большое простое число P и большое целое число G, причем G < P. Числа P и G могут быть распространены среди группы пользователей.»

«Затем выбирают случайное целое число X, причем X<P. Число X является секретным ключом и должно храниться в секрете.»

«И вычисляют $Y = G^X \bmod P$. Число Y является открытым ключом.

Для того чтобы зашифровать сообщение M, выбирают случайное целое число K, 1< K< P –1, такое, что числа K и (P –1) являются взаимно простыми.

Затем вычисляют числа

$a = G^K \bmod P$,

$b = Y^K M \bmod P$.

Пара чисел (a,b) является шифртекстом. Заметим, что длина шифртекста вдвое больше длины исходного открытого текста M.

Для того чтобы расшифровать шифртекст (a,b), вычисляют

M = mod P. (∗)

Поскольку

$a^X \equiv G^{KX} \bmod P$,

то соотношение (*) справедливо.

П р и м е р. Выберем P=11, G=2, секретный ключ X=8. Вычисляем

$Y = G^X \bmod P = 2^8 \bmod 11 = 256 \bmod 11 = 3$.

Итак, открытый ключ Y=3. Пусть сообщение M=5. Выберем некоторое случайное число K=9. Убедимся, что НОД (K, P–1) =1. Действительно, НОД (9, 10) =1. Вычисляем пару чисел a и b:

$a = G^K \bmod P = 2^9 \bmod 11 = 512 \bmod 11 = 6$,

$b = Y^K M \bmod P = 3^9 \cdot 5 \bmod 11 = 19683 \cdot 5 \bmod 11 = 9$.

Получим шифртекст (a, b) = (6, 9). Выполним расшифрование этого шифртекста. Вычисляем сообщение M, используя секретный ключ X:

$M = b/a^X \bmod P = 9/6^8 \bmod 11$.

Выражение $M = 9/6^8 \bmod 11$ можно представить в виде $6^8 M \quad 9 \bmod 11$ или $1679616 * M \quad 9 \bmod 11$. Решая данное сравнение, находим M = 5.»

2 Методы приведения чисел по модулю

Возведение в степень по модулю – одна из действий над числами выполняемая по модулю. Примеряется в криптографии. Есть много методов формирования остатков при делении на модуль. Если использовать двоичное представления целых положительных чисел можно выделить три способа формирования остатков по произвольному модулю Р. В первом способе кратные модули Р*i (i=1,3…k) формируются в разных блоках, затем они с использованием К сумматоров одновременно (параллельно) вычитаются из приведенного числа А. Наименьший положительный остаток Ci=A-P*i является результатом. Такой способ формирования остатков характеризуется большими аппаратными затратами - при больших соотношениях приводимого числа А и модуля Р сложность схемы резко возрастает. Этот способ приемлем по аппаратным затратам лишь при малых значениях А и Р. Второй способ основан на последовательном формировании остатков (ri) разрядных весов двоичного числа (2i) от деления на модуль Р с дальнейшим суммированием по модулю Р тех остатков, для которых коэффициенты Ai соответствующих весов равны единице и реализуется по формуле: A $mod\ P$ = ($\sum$ (2 $imod\ P$)Ai)$mod\ P\ .\ k-1$ 0 Так как для двоичной системы счисления коэффициенты Ai (i=0÷k-1), принимают только два значения (0 и 1), то суммируя заранее вычисленные частичные остатки по модулю от числа 2i (i=0,1,…k-1) для тех i, для которых коэффициенты Ai=1, получают остаток по модулю Р от числа А. Так как для двоичный системы счисления коэффициенты a(i=0,,K-1)принимается только болевые значение сложением заранее вычисленные остатки по модулю Р от числа А. Частичный остаток 2^0 для любого модулю (Р>2) всегда равен 1.ЧО от 2^1 в два раза превышает ЧО 2^0 таким образом частичный остаток 2^i в два раза превышает 2^{i-1}.Аксиомой этого метода является вычисление в умножении на два частичного остатка 2^{i-1} и приведение числа по модулю А. Операция умножения на 2 может быть реализована сдвигом влево. Операция приведение по модулю Р для чисел, не превышающих 2Р-1 реализуется по другому. Если число не превышает величину 2Р-1 из него вычитается модуль Р,а результат является остатком.

В 3-ем способе модуляции применяется принцип метода машины двоичного разделения со смещением остатков налево. Модуль Р поочередно вычитается, начиная с самых больших цифр А. На любом шаге вычитания складывается грядущий выборочный остаток. Дабы определить грядущий выборочный остаток, предшествующий остаток двигается налево на 1 цифру, а грядущая цифра количества А прибавляется к младшему означающему биту выборочного остатка. И модуль вычитается из приобретенного номера. Выборочные останки образуются в PSF выборочных остаточных форм. Композиция всех выборочных невязок сформирует матричную схему для конфигурации количества А по модулю Р. Дефектом первого способа считается надобность владеть делитель двойной длины и регистр делителя. 2

способ разрешает для вас получать узлы одинарной длины; в следствие этого мы не станем рассматривать 1-ый способ разделения.

Если числа A и P положительны, то частное Q и остаток R будут положительными. Последовательный алгоритм деления сдвигает число A и вычитает число P от A до тех пор, пока не будет найден остаток R, удовлетворяющий условию 0<R<n. При этом не исключено получение отрицательного остатка после вычитания.

Разделение чисел может быть выполнено с восстановлением или без восстановления остатков. В этом случае делитель включает в себя схему «исключающее ИЛИ», которая обеспечивает передачу делителя на вход сумматора либо в прямом, либо в обратном коде, в зависимости от знака следующего баланса. Это приводит к усложнению схемы деления устройства.

Деление может быть сделано двумя способами:

1) с фиксированным делением и смещением делителем вправо;

2) с фиксированным делителем и смещенным влево делителем.

В аппаратной реализации модуля сокращения могут использоваться различные подходы, которые приводят к множеству структур устройства для получения оставшейся части разделения модуля. Эти структуры представлены в различных публикациях, но не систематизированы и не проанализированы. Анализ структур и принципов функционирования различных модульных устройств позволил выявить их характерные особенности:

1) последовательное или параллельное выполнение операций возведения в квадрат и извлечения остатков от деления на модули;

Operation управление устройством одним касанием или несколькими часами;

Наличие или отсутствие цепи управления (управления двигателем) через процесс восстановления на модуле;

2) и спользование определенной системы счисления.

Благодаря этим характеристикам все модульные устройства можно разделить на классы. Ниже приведена классификация модульных устройств на основе вышеуказанных критериев.

Классификация по степени параллелизма процессов умножения и редукции модуля продукта:

1) Параллельный - сокращение модуля происходит параллельно в процессе умножения. После того, как каждый субпродукт был получен каждый раз, его абсолютное значение уменьшается, и в будущем субпродукт, но его остаток, не используется для продолжения репликации.

2) последовательная - модульная редукция выполняется последовательно при получении работы. Умножение на a или монтаж и квадратуру выполняется только тогда, когда модуль обнаружит остаток от деления.

Классификация по количеству циклов, необходимых для получения остатка в разливочном устройстве, по модулю:

1) многоцикловые устройства, где остаток определяется путем многократного вычитания из исходного сводимого числа, а затем из результирующих положительных невязок модуля, в соответствии с которым выполняется восстановление. И здесь возможны два варианта: все вычитания реализуются на одном и том же узле, который многократно повторяет циклы в процессе получения каждого остатка (циклическая организация), а вычитания реализуются на аппаратном (конвейерном) спонсоре, каждый из которых схема используется только один раз. , Каждый остаток формируется на уровне его производства, количество которого определяется максимальным количеством положительных остатков.

2) Несимметричные устройства, в которых вычитания выполняются параллельно из сводимого числа модуля P и нескольких чисел модуля (2P, 3P, 4P)

3) Получено несколько остатков, результатом является наименьший положительный остаток.

Классификация по наличию блока автоматического управления (УА) в литейной машине по модулю:

1) Комплексное устройство - представлено в виде серии управляющих и управляющих машин (ОА и УА). UA генерирует управляющие сигналы и управляет процессом сокращения в модуле, а все операции выполняются в ОА. Машина оператора, в свою очередь, отправляет информационные машины на машину управления, которые служат руководством для машины управления при генерации следующего сигнала управления. Это типичный случай традиционной панели управления оператора (OU), для синтеза которой применимы известные методы синтеза цифровых автоматов, включая микропрограммные машины (MPA). Возможны следующие варианты: Блок управления может быть выполнен в виде схемы UA с жесткой логикой; - Блок управления может быть построен по принципу программного управления - UA с программируемой логикой;

2) Автономное устройство - управляющая часть не назначена, все реализовано в виде единой схемы, управляющие сигналы формируются в результате операций.

Классификация по системе счисления, используемой в устройстве приведения по модулю:

1) двоичная система счисления;

2) двоично-десятичная система счисления;

3) вспомогательные системы счисления с основанием 2h, где h целое число и h>=2. Переход к вспомогательной системе счисления осуществляется условно из двоичной системы счисления путем разбиения двоичного числа на диады (h=2, 2 h =4), на триады (h=3, 2 h =8), на тетрады (h=4, 2 h =16) и т.д.

Способ формирования остатка путем параллельного вычитания чисел кратных модулю A

Однотактовое устройство приведение чисел характеризуется большими аппаратными затратами. В таких устройствах параллельно разные блоки

формируется кратные модули PxI (где i=2,3,…k). Затем модуль P и сформированные кратные модули 2p,3p…,kp с использованием к сумматоров и одновременно вычитается число A .Наименьший положительный остаток R=A+P+1 является результатом. Для формирование кратных 2p , 3p,…kp требуется К-1 сумматоров. С увеличением числа div = $\frac{\mathbf{A}}{\mathbf{P}}$ резко увеличивается число сумматоров для вычисления значения остатка и формирователей кратных i×p. Если взять div= 6 для формирования кратных p,2p….6p потребуется 6 сумматоров и 3 формирователя кратных 3$\bar{P}$ 4$\bar{P}$ 5$\bar{P}$.

Количество сумматоров Ncm=1,5(Nkp+N)=1,5KNсм

При делении числа A на число P нас интересует не частное Q ,а остаток R.Для данных делимого A и делителя P частное Q и остаток R вычисляется так чтобы выполнялось соотношение

$$A=Q*P+R \qquad (2.1)$$

Недостатком первого случая является нужно иметь устройство деление сумматор и регистр делителя двойной длины. Второй же способ позволяет обойтись узлами одинарной длины. Если число A P положительны то частное Q то остаток R будут положительными. Последовательный алгоритм сдвигает до тех пор, пока не будет найден остаток R. Подходящую условию $0 \le R < n$.Однако может получиться отрицательный остаток именно поэтому отличается деление с восстановлением остатка и без восстановления остатка.

2.1 Деление с неподвижным делимым и сдвигаем право

В ЭВМ операция деление чисел с помощью соответствующих алгоритмов сводится к операциям вычитания и сдвига. Реализовать деление можно двумя способами как уже оговаривалось выше. Расмотрим случай на примере.

Пусть

$$Z=X/Y \qquad (2.2)$$

X- делимое ,представляемое словом(2n-1)

Y- делитель

Z – частное содержащими n-1 цифровых разрядов.Для обобщения оговариваем что числа которые делятся ,предаставляется в коде .Так как Z частное ((n-1) разрядное число то диапазон от 0 до 2^{n-1} .Это возможно только при (| X| - |Y|)<0 |Y| = |Y| *2 $^{(n-1)}$. Для получения (| X| - |Y|) следует отнять из |X| делитель |Y|,выровняв их так что бы разряд Y был под n – м разрядом делимого. Это возможно получить сдвинув делитель Y относительно делимого X на n-1 разрядов влево.

Если результат вычитания (| X| - |Y|) (это вычитание называют пробным) больше 0, то $Z > 2^{n-1}$ и деление невозможно если меньше 0, то возможно выполнить деление. Недостатком такого способа является двойная длина СМ и его регистров в АЛУ.Рассмотрим пример:

X = -38 Y = 7. Представим делимое и делитель в прямом коде старший разряд знаковый который в плюсе равен 1 а минусе 0.$X_{пр}$=10100110,Y = 0111, тогда модуль делимого и делителя в их старших разрядов заносятся в нули. Частное Z должно быть представлено в коде с 4 двоичными разряда .Выполняем деление 10100110/0111. В соответствии с правилами деления очередной цифрой частного является 1 ,если после вычитания из остатка делителя получается положительный результат, и 0 если результат отрицателен.

Деление с неподвижным делителем и сдвигаемым влево делителем

Этот метод позволяет создавать ALU с n-битными регистрами и сумматорами. Этот метод имеет два типа:

1) Деление с неподвижным с восстановлением осткатков

2) Совместное использование с фиксированным делителем без восстановления остатков

Разделение с извлечением остатка может быть разложено следующим образом:

1) Начальное значение частичного остатка зависит от высокого разряда делимого

2) частичный остаток удваивается путем перемещения разряд влево.

3) делитель вычитается из смещенного частичного остатка

4) модуль является положительным, если число равно 1, и 0, если отрицательное. В 0 остаток возвращается к значению до вычитания.

Разделение без восстановления отставания может быть решено следующим образом.

1) Предполагается, что начальная значение остатка равна старшему разряду делимого.

2) Частичный остаток удваивается и смещается на 1 влево

3) делитель вычитается из частичного остатка, если остаток является положительным при добавлении отрицательного делителя

Недостатком алгоритмов, описанных выше, является необходимость выполнения дополнительных операций сложения за один шаг для восстановления остальных. Эти методы увеличивают время деления, которое может варьироваться в зависимости от комбинации кодов операндов. По этим причинам реальные делители строятся на базе без восстановления отставания.

2.2 Деление с восстановлением остатков

Наиболее очевидным алгоритмом является алгоритмом деления с фиксированным делителем и восстановлением остатка. Это связано с тем, что он очень похож на обычный метод деления на полосу. Этот алгоритм можно описать следующим образом.

1) Предполагается, что начальное значение частичного остатка (ЧО) равно наибольшим разрядам делимого

2) Делитель вычитается из частичного остатка и анализируется остаточный символ.

3) Если остаток положительный, деление невозможно, формируется символ переполнения и процесс завершается, в противном случае остаток восстанавливается путем добавления делителя, и деление продолжается.

4) Частичное смещение сдвигается на одну позицию влево, а следующая цифра делимого вводится в нижнюю цифру регистра рстатка, которая высвобождается во время сдвига.

5) Делитель вычитается из сдвинутого остатка и анализируется знак результата вычитания.

6) Следующая цифра модуля детали равна единице, если результат вычитания положительный, и нулю, если он отрицательный. В последнем случае CR сбрасывается до значения перед вычитанием.

7) Пункты с 4 по 6 выполняются последовательно для получения всех цифр факторного модуля.

На рисунке 2.1 выделен процесс деления и восстановления остатка, делимым является 41, а делитель 7.

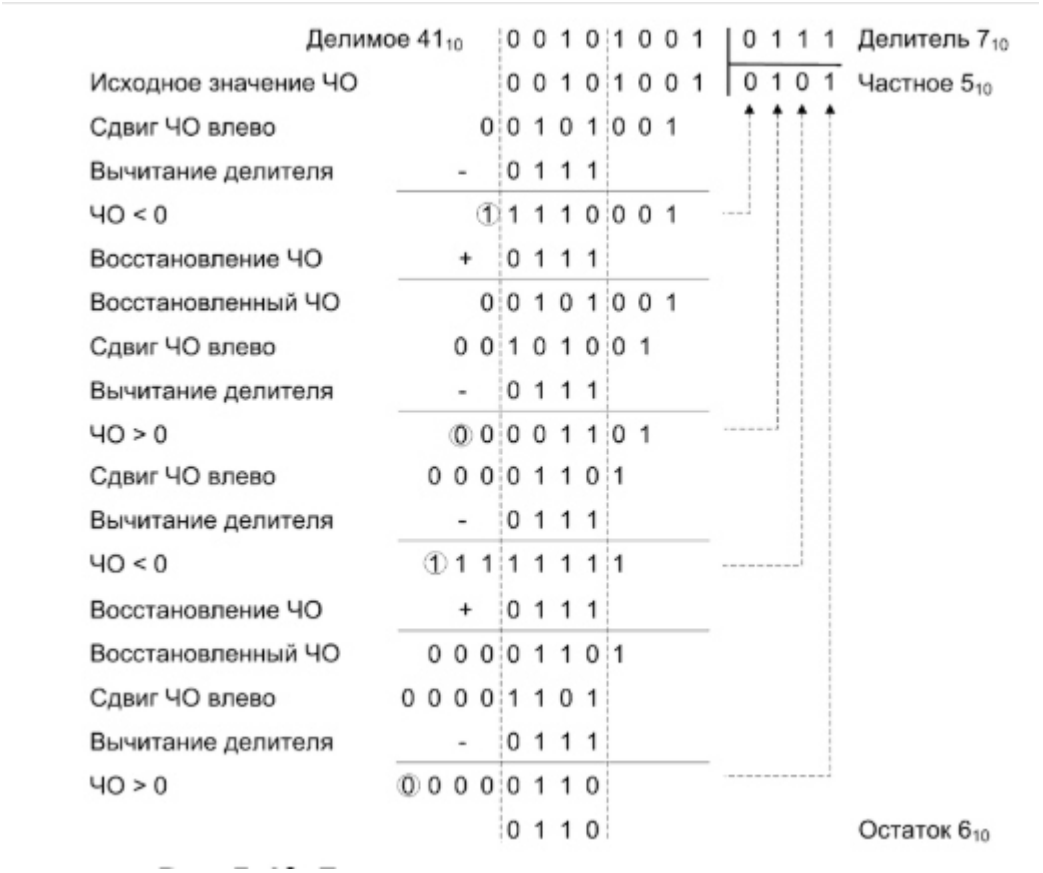

Рисунок 2.1 – Деление с восстановлением остатка

Деление без восстановления остатков

Недостатком описанного метода является необходимость выполнения дополнительных хирургических опор на отдельных этапах для

восстановления остатка образца. Это увеличивает время выполнения деления, которое также может варьироваться в зависимости от конкретной композиции кодов операнда. По этим причинам реальные разделители построены на основе метода разделения с фиксированным разделителем, без восстановления остальных. При этом пункты 1-4 и 7 полностью соответствуют соответствующим элементам предыдущего алгоритма подразделения, а пункты 5 и 6 сформулированы следующим образом:

1) Делитель вычитается из смещенного частичного остатка, а остаток добавляется к смещенному частичному остатку, когда остаток отрицательный.

2) следующая цифра модуля частного блока, если остаток операции (сложение или вычитание) положительный, и ноль, если он отрицательный. Деление без сохранения остатка показано на рисунке 2.2

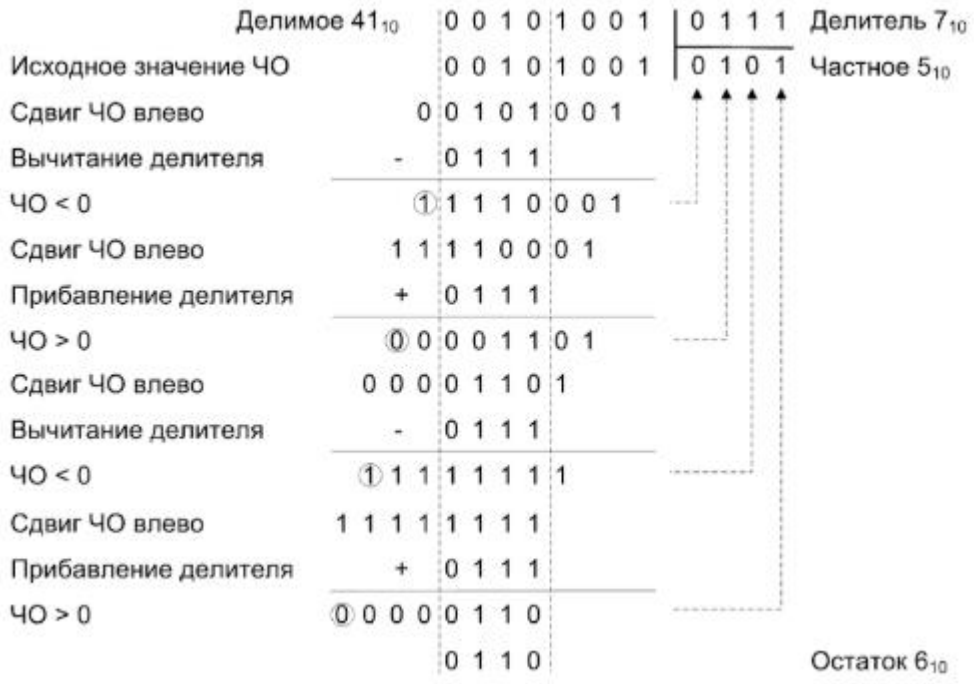

Рисунок 2.2 – Деление без восстановления остатка

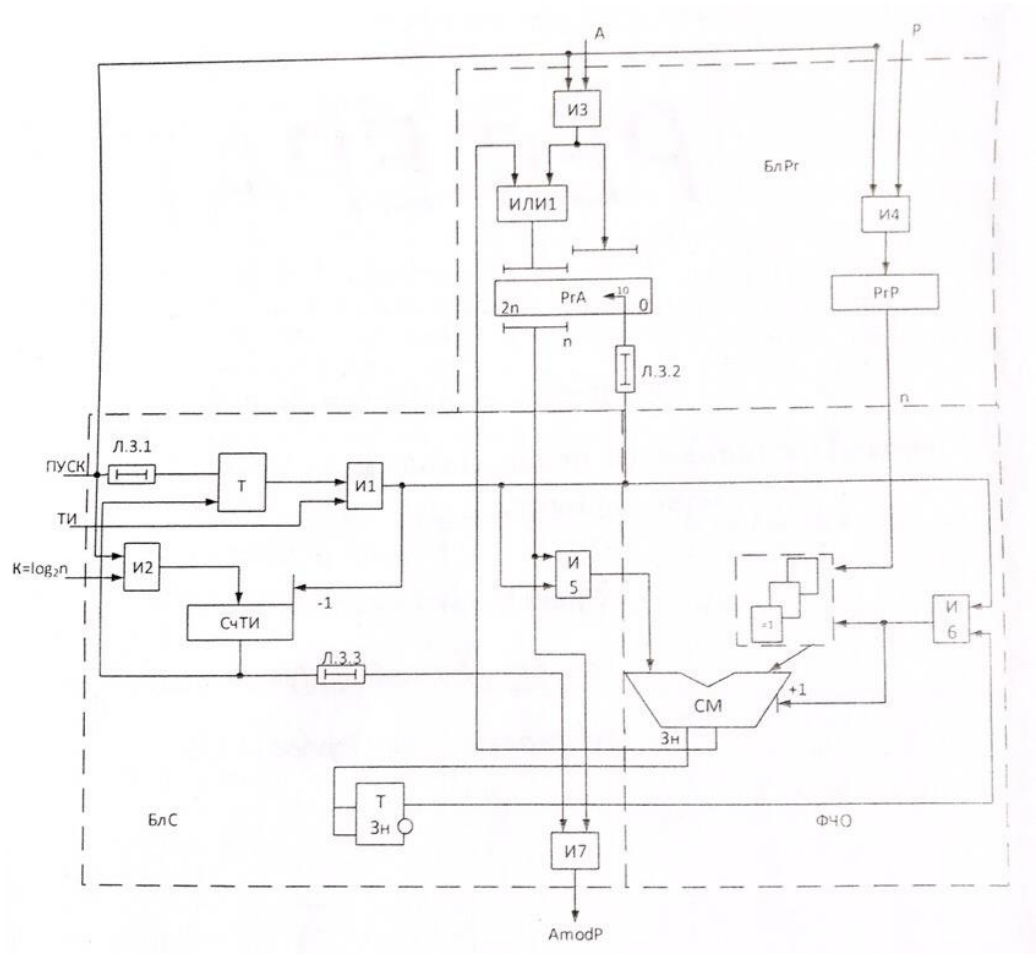

Рисунок 2.3 – Устройство приведения числа А по модулю Р, построенное по алгоритму без восстановления остатка

Тактовый импульс поступает на схему И6, на второй вход которого подается «0» из единичного выхода триггера знака ($T_{зн}$). Сигнал «0» с выхода И6 подается на вход блока схемы «исключающего ИЛИ» подается прямой код делителя – модуля Р. Поскольку первоначально из триггера знака поступает уровень «0», то на выходе схемы «исключающего ИЛИ» формируется обратный код модуля Р. На выходе сумматора формируется первый частичный остаток $r_1=r_0+P+1$

r_1 через схему ИЛИ записывается в Рг $[2_{n+1}+n]$, а знак результата в триггер знака. После чего ТИ1 через Л3.2 поступает на сдвигающий вход РгА и сдвигает его на один разряд влево. На этом заканчивается действие тактового импульса ТИ1.

С поступлением импульса ТИ2 показание СчТИ уменьшается еще на единицу. Сдвинутый частичный остаток $2r_1$ подается через схему И5 на вторые входы сумматора, а на вторые выходы поступает модуль в прямом коде, $T_{зн}=1$ (отрицательный остаток) или обратном коде, если $T_{зн}=0$ (положительный остаток) При этом на сумматоре формируется $r_2=2r_1+P+1$ при положительном остатке, либо $r_1=2r_1+P$ при отрицательном остатке. Затем r_1 с выходом СМ записывается в РгА и сдвигается на один разряд влево.

После поступления n-го тактового импульса СчТИ обнуляется из 43 удвоенного П-1-го частичного остатка в зависимости от знака предыдущего остатка вычитается или суммируется делитель (модуль) и результат записывается РГА. НА время формирования последнего остатка сигнал «Конец операции» который формирует СчТИ при его обнулении остаток выдается на выход схемы И7.

2.3 Оценка эффективности существующих алгоритмов и методов шифрования

При сравнительном анализе алгоритмов шифрования следует учитывать следующие особенности:

- практическая сила шифрования;
- потребление ресурсов и энергоемкость;
- рабочая скорость.

Алгоритмы шифрования разработаны так, чтобы требовать раскрытия для поиска в пространстве ключей, поэтому надежность шифрования определяется длиной ключа.

Существует два класса методов шифрования: симметричный и асимметричный. В первом случае и получатель, и отправитель информации используют один и тот же ключ шифрования. Во втором случае отправитель имеет закрытый ключ шифрования, а получатель имеет открытый ключ для расшифровки.

В случае симметричной схемы шифрования субъект каким-то образом должен предоставить свой собственный ключ всем другим участникам переговоров, и общее количество используемых ключей достаточно велико для большего числа участников переговоров. Внедрение асимметричного метода требует только распространения раскрытых ключей всем подписчикам, то есть чистого количества ключей таким же образом, как и количество участников в обмене. На практике раскрытые ключи имеют все шансы быть сохраненными в специальной базе данных. Если вам нужно отправить зашифрованные сообщения своему партнеру, вы можете сначала отправить запрос на его искренний источник. После получения вы можете запустить программу шифрования и отправить результат ее работы адресату. Например, реализация раскрытых ключей основана на электронной подписи, которая, несомненно, позволяет идентифицировать отправителя. Подобные инструменты могут быть использованы для предотвращения изменения сообщения на пути от отправителя к получателю.

Методы симметричного шифрования включают в себя следующие алгоритмы: Blowfish, DES, 3DES, CAST, AES, GOST. Асимметричными являются: RSA, Эль-Гамаль.

Алгоритм шифрования Blowfish был основан в 1993 году Брюсом Шнайером. В общем случае алгоритм состоит из двух этапов - расширение ключа и шифрование / дешифрование исходных данных. Сложная схема генерации ключей затрудняет атаку на алгоритм, если вы пытаетесь взломать

его с помощью грубой силы. Однако это делает его непригодным для систем, в которых ключ часто меняется, а небольшие данные шифруются для каждого ключа. Алгоритм работает лучше всего для систем, которые шифруют большие поля данных одним и тем же ключом.

Алгоритм шифрования DES был основан в 1975 году IBM. С 1977 по 2001 год это был федеральный стандарт США для шифрования. Алгоритм симметричного шифрования, который использует ключ как для получателя, так и для отправителя, т.е. этот ключ используется как для расшифровки, так и для шифрования. DES имеет 64-битные и 16-часовые сети для сети Feistel и использует 56-битный ключ для шифрования. Алгоритм использует комбинацию нелинейных S-блоков и линейных преобразований. Основным недостатком является то, что размер ключа составляет всего 56 бит, что недостаточно для текущего состояния разработки компьютера.

Алгоритм шифрования Triple DES (3DES) представляет собой симметричное блочное шифрование, разработанное в 1978 году на основе алгоритма DES для устранения основного недостатка последнего - небольшой длины ключа (56 бит), которая может быть взломана с помощью грубой силы. Скорость 3DES в три раза ниже, чем у DES, но надежность намного выше. С 3DES недостатки DES могут быть легко устранены [3].

Алгоритм шифрования CAST в некотором смысле аналогичен DES. Этот алгоритм основан на шести S-блоках с 8-битным входом и 32-битным выходом. Алгоритм сложен и зависит от реализации. Главной особенностью алгоритма CAST является то, что блоки не установлены. Используются 128 и 256-битные ключи.

Метод шифрования AES (Rijndael) был разработан в 1997 году и в настоящее время считается федеральным стереотипом шифрования в США. Основой этого метода является симметричное блочное шифрование, которое работает с блоками длиной 128 бит и использует ключи длиной 128, 192 и 256 бит. Метод может работать с блоками и ключами разной длины, но они не интегрированы в стереотип. Шифрование в методе AES использует правильные методы преобразования данных: ExpandKey - Определить ключи округления для всех раундов. SubBytes - заменить байты поисковой таблицей; ShiftRows - повторное смещение строк в форме на разные значения; MixColumns - смешивание данных в любом столбце формы; AddRoundKey - добавляет круглый ключ с формой.

Алгоритм шифрования ГОСТ был установлен в 1989 году в СССР и стал Федеральным стандартом шифрования Российской Федерации. Сердцем алгоритма является сеть Фейстеля. Использует 128-битный ключ шифрования и является надежным. Скорость работы довольно низкая, но вы можете увеличить скорость работы, потому что вы можете изменить настройки и в то же время уменьшить силу шифрования.

Алгоритм шифрования RSA (Rivast, Shamir and Adelman, 1977) предполагает, что переданное зашифрованное сообщение может быть прочитано только адресатом. Этот алгоритм использует два ключа - открытый

и закрытый. Этот алгоритм привлекателен, даже когда большое количество субъектов должны общаться по схеме «все со всеми».

Криптосистема Рабина (М. Рабин) является вариантом криптосистемы RSA. RSA основан на сравнительных исследованиях. Криптосистема Рабина основана на квадратичных сравнениях и может быть представлена как криптосистема RSA, в которой значениям e и d присвоены значения e = 2 и d = 1/2. Другими словами, шифрование - c = p2 (mod n), дешифрование - P = C1 / 2 (mod n).

Открытый ключ для доступа в криптосистеме Рабина - n, секретный ключ - кортеж (p, q). Любой может зашифровать сообщение с помощью n, но только Боб может расшифровать сообщение с помощью p и q. Расшифровка сообщения невозможна для Евы, потому что она не знает значения p и q. Рисунок 2.4 показывает шифрование и дешифрование.

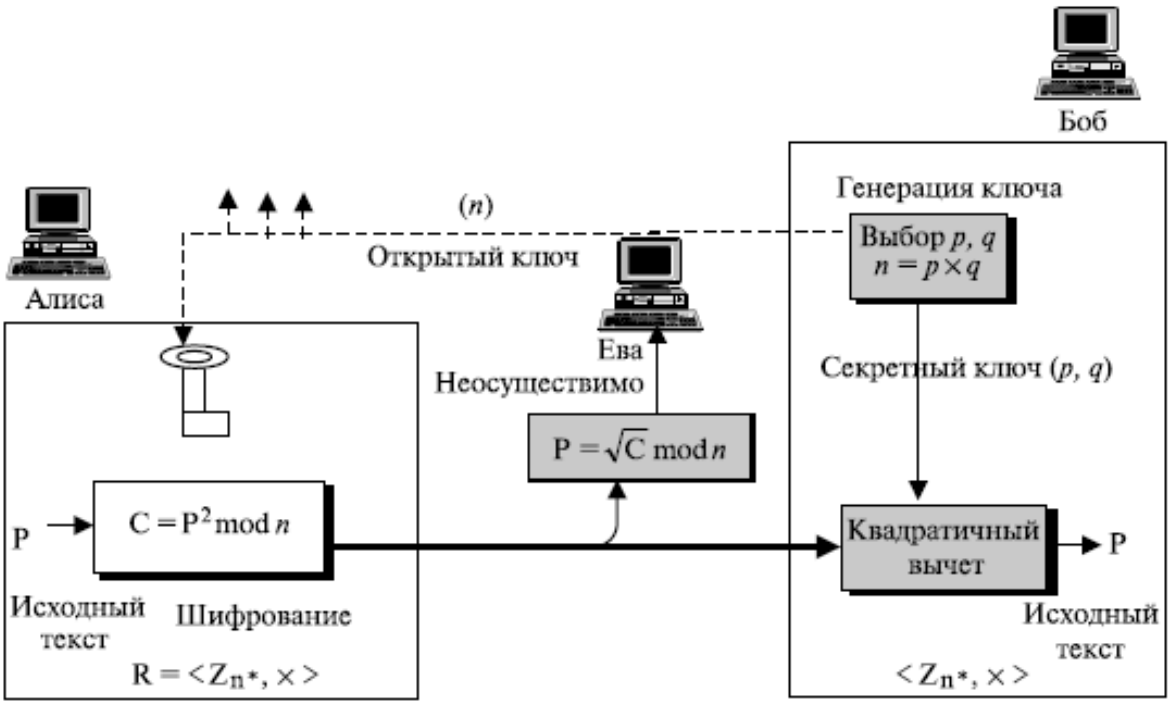

Рисунок 2.4 – Шифрование, дешифрование и генерация ключей в криптосистеме Рабина

Следует подчеркнуть, что Боб при использовании RSA может сохранять и отклонять d и n после генерации ключей из p, q и φ (n). Если Боб использует криптосистему Рабина, он должен сохранить p и q.

Криптографическая система Рабина безопасна, а p и q - большие числа. Сложность криптографической системы Рабина такая же, как сложность процесса факторизации большого числа n в двух простых факторах p и q. Другими словами, криптографическая система Рабина так же безопасна, как и RSA.

Алгоритм шифрования Эль-Гамаля был основан в 1985 году Эль-Гамалем. Алгоритм решает все три основные задачи: шифрование данных, создание цифровой подписи и определение общего ключа.

Кроме того, возможны изменения схемы проверки пароля, проверка личности сообщения и другие параметры. Безопасность этого алгоритма, а также алгоритма Диффи-Хеллмана основана на сложности вычисления дискретных логарифмов. Этот алгоритм фактически использует схему Диффи-Хеллмана для генерации общего секрета для подписчиков, отправляющих друг другу сообщение. Затем сообщение шифруется путем умножения его на этот ключ.

В научной литературе приводятся примеры раскрытия источников: почти каждая зашифрованная телеграмма на Ближний Восток начиналась со списка многочисленных и известных областей адресата, используемых для расчета гаммы, иногда с открытым шифром и телеграммой. чтение было быстрее, чем ранее достигло адресата.

Криптоаналитик не только имеет доступ к зашифрованному тексту и открытым текстам, но также имеет возможность выбора открытого текста для шифрования. Таким образом, криптоаналитик может выбирать блоки для шифрования, анализ которых дает больше информации о ключе.

Подобные атаки были направлены против немецких шифров: союзники преднамеренно выдавали определенную информацию для получения зашифрованного текста или провоцировали сообщения о событиях в городах с уникальными именами, которые служили особенно хорошими хлевами.

Криптоаналитик может выбрать другой зашифрованный текст для расшифровки и имеет доступ к дешифрованному открытому тексту. Например, криптоаналитик имеет доступ к «черному ящику», который выполняет дешифрование. Его работа состоит в том, чтобы получить ключ.

Злоумышленник (слово «криптоаналитик» здесь не совсем применимо) угрожает, шантажирует или подвергает пыткам пользователя системы, пока он не получит ключ. Открытие при покупке ключа называется взяткой за получение ключа. Тот же запрос о выдаче ключей может быть привлечен к ответственности. [22, с. 37]

Существование этих методов взлома требует создания многосторонних протоколов, в которых никто из пользователей не обладает всей важной информацией, или использования стеганографии, чтобы скрыть факт передачи секретной информации.

Исходя из описанных характеристик атак, оптимальная криптосистема должна решать следующие задачи защиты информации:

– обеспечение конфиденциальности информации;
– обеспечение целостности информации;
– обеспечение достоверности информации;
– обеспечение быстрого доступа к информации;
– обеспечение юридической значимости информации в форме электронного документа;
– Обеспечение прослеживаемости действий клиента.

Конфиденциальность - это свойство информации, доступной только ограниченному числу пользователей информационной системы, в которой эта информация циркулирует.

Целостность - это свойство информации или программного обеспечения поддерживать свою структуру и / или содержание во время передачи и хранения.

Подлинность (достоверность) - это свойство информации, которая выражается в целостности и в строгой связи с объектом, из которого она исходит, или объектом, из которого эта информация получена.

Эффективность - способность информации или информационных ресурсов быть доступными для конечного пользователя в соответствии с его требованиями времени.

Юридическая ценность - означает, что документ имеет юридическую силу. Для этой цели компании, которым требуется подтверждение юридической значимости, соглашаются принять определенные атрибуты информации, которые выражают их правоспособность. Например, при введении электронных цифровых подписей. [9, с. 39]

Не отслеживаемость - это способность незаметно выполнять определенные действия в информационной системе для других объектов, включая администраторов. Это требование предназначено для предотвращения полного мониторинга пользователей IP.

Конфиденциальность обеспечивается с помощью шифрования, целостности и аутентичности - с помощью EDS и MAC (в зависимости от цели), юридическая значимость - с помощью EDS. Примером решения проблемы прослеживаемости могут быть электронные системы голосования.

Электронная (цифровая) подпись (ЭЦП) - это криптографическое преобразование, которое прикрепляется к тексту и позволяет проверить авторство и целостность сообщения при получении текста другим пользователем. Для создания EDS используются закрытый ключ отправителя и подтверждение открытого ключа.

Имитационная защита - защита от наложения ложных данных. Для защиты от имитации к зашифрованным данным добавляется имитатор (или MAC - Message AuthenticationCode - это код аутентификации сообщения). Это последовательность данных фиксированной длины, извлеченных из открытых данных и закрытого ключа в соответствии с определенным правилом. [3, с. 10]

3. Проектирование устройства умножения по модулю на делительных устройствах с восстановлением остатков

3.1 Устройство умножения по модулю на делительных устройствах с восстановлением остатков

При проектировании аппаратных и программно-аппаратных криптосистем с открытым ключом становится актуальной разработка эффективных схем для реализации одной из основных операций - изменения числа.

Алгоритм привдения чисел по модулю может быть реализован при помощи устройства, схема которого приведена на рисунке 3.1.

Процедура начинается с занесения делимого A в 2n-разрядный регистр делимого (PpA), роль которого исполняет n-разрядный регистр остатка (PrR). Делитель записывается в n-разрядный регистр делителя.

В каждом шаге содержимое PrR сдвигается на один разряд влево. В зависимости от сочетания знаков частичного остатка и делителя определяется значение очередной цифры частного и требуемое действие: вычитание или прибавления делителя. Операция вычитания заменяется прибавлением делителя, взятого с обратным знаком и представленного в виде дополнительного кода. Изменение знака и преобразование в дополнительный код реализуется путем передачи делителя н вход сумматора обратным кодом. (инвертирование обеспечивает схемы исключающего ИЛИ на одном из входов сумматора) с последующим добавлением единицы к младшему разряду сумматора. Цифра очередная частного записывается в освободившийся при сдвиге младший разряд. Содержимое циклов счетчика уменьшается на единицу.

Процедура повторяется до того момента пока все цифры делимого не исчерпаются. По окончании операции деления частное находится в регистре частного, а остаток от деления будет находиться в регистре остатка.

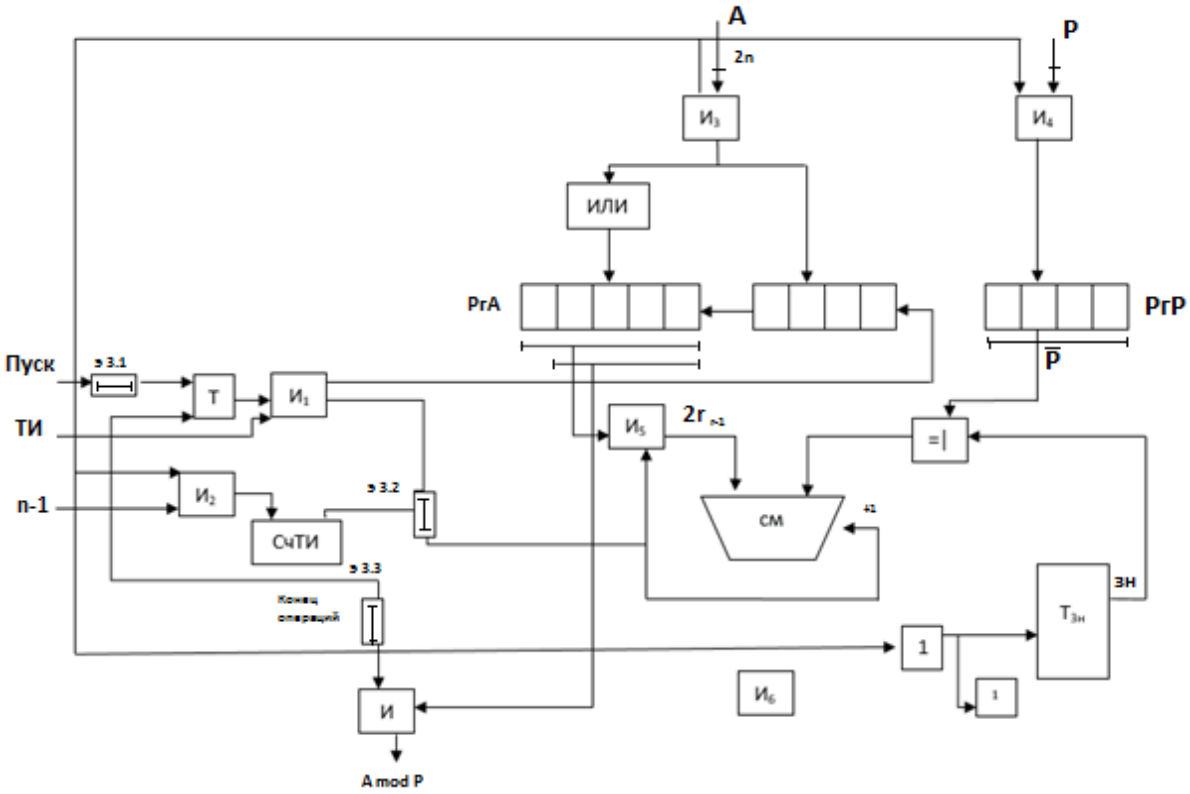

Рисунок 3.1 – Устройство приведения чисел по модулю на основе делительного устройства без восстановления остатков.

3.2 Структура устройства

Счетчик команд – неотлиемлимый объект устройства управление ВМ. Ск-выполняет важнейшую функцию. Счетчик команд заносит адрес ячейки основной памяти где хранится команда которая должна выполнится первой. В рассматриваемой ВМ любая команда занимает одну ячейку поэтому содержимое увеличивается на 1 что обеспечивает подачу сигнала .По завершению текущий команды адрес следующий команды всегда берется из СК. Для изменения естественного порядка вычислений надо занести в СК точки перехода.

Адресный регистр - используется для хранения адресов операндов.

Сумматор устройства является логическим рабочим узлом, который выполняет арифметическое сложение двоичных, троичных или nn-ичных кодов. Может складывать два (бинарный), три (тернарный) или nn чисел (nn-арный). Помимо сложения выполняются и другие операции: учёт знаков чисел, выравнивание порядков слагаемых.

3.3 Пример работы схемы

$P = 14_{10} = 01110_2$ (2*7=14)

$A = 185_{10} = 1011001_2$

R= A mod P= 185 mod 14 = 185-]185/14[*14 = 185 –]13[*14 = 185-182 = 3

Необходимо найти остаток:

(1011001_2) mod1110_2= 0011; количество шагов = 4, то есть необходимо взять r_1-r_4

$2r_0$=10111 = 16+7 = 23_{10}

r_1 = 23-14 = +9 ~ Зн=0, П=1 в следующем шаге из $2r_1$ вычитаем Р=14

$2r_1$ = 18+a_2 = 18

r_2 = 18-14=4 ~ Зн = 0, П=1 в следующем шаге из $2r_1$ вычитаем Р=14

$2r_1$ = 8+a_2 = 8

r_3=$2r_1$-14 = 8-14 = -6 ~ Зн = 1, П=0 передача в РгА блокируется

-6 передается в РгА, затем сдвигается влево на один разряд и к сдвинутому остатку присоединяется a_0=1, тогда в РгА формируется остаток $2r_3$+a_0= -12 + 1 = -11; Поскольку в триггере знак находится в состоянии «0» (потому что П=0), то на упр. Вход схемы = 1 становится уровня «0»

При этом на входе схемы = 1 формируется Р, который суммируется с -11+14 = 3, что и является результатом на выходе СчТИ, формируется сигнал конец операции, который через схему $И_6$ выдается на выход.

$2r_3$+a_0 = -12+1 = - 11 + 14 = 3

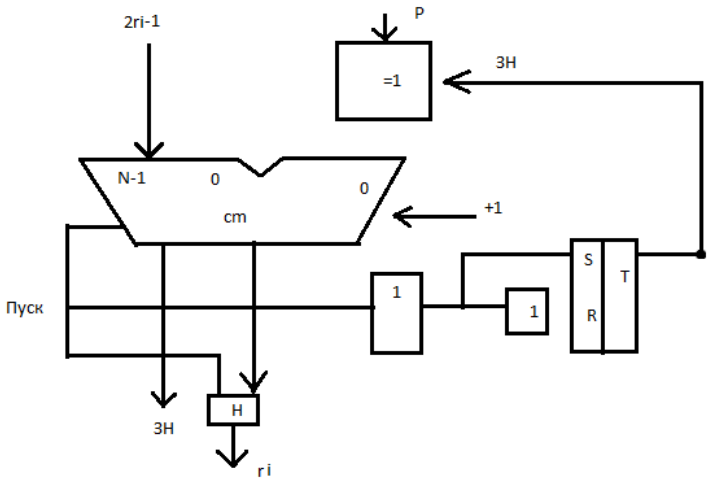

Рисунок 3.2 – структура ФЧО

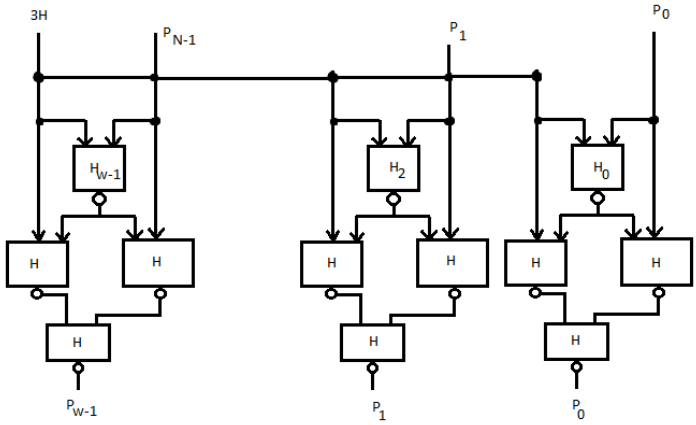

Рисунок 3.3 – Функциональная схема блока «исключающее ИЛИ»

3.4 Конвейерная схема приведения чисел по модулю

В матричной схеме уменьшения количества модулей существует важный потенциал для повышения производительности возможности конвейерной обработки. Во время конвейерной обработки весь процесс модульности делится на последовательность завершенных шагов. Каждый из этапов процедуры уменьшения модуля выполняется на своем собственном этапе конвейера, причем все этапы работают параллельно. Результаты, полученные на i-й ступени, передаются на дальнейшую обработку в (i+1)-ю ступень конвейера. Перенос информации со ступени на ступень происходит через буферную память, размещаемую между ними. Синхронность работы конвейера обеспечивается тактовыми импульсами, период которых τ определятся самой медленной ступенью конвейера и задержкой в элементе буферной памяти. На рисунке С. 14 приведена конвейерная схема приведения числа по модулю, построенная на основе матричной схемы. Конвейер состоит из трех ступеней. Каждая ступень состоит из: ФЧО; буферных регистров частичного остатка; регистров РгЗР и РгР; разрядов числа А, еще не вступивших в операцию. Конвейер управляется тактовыми импульсами ТИ. После заполнения конвейера при подаче каждого тактового импульса на выходе формируется результат пары Ai и Pi.В архитектуре множества вычислительных проектов где конвейеризация приносит ощутимый прирост вычислительных систем. По степени конвейеризации конвейеры могут синхронными и асинхронными. Синхронные конвейеры обычно используют в ВМ. Повысить производительность процессора можно за счет параллельного выполнения отдельных этапов рабочего цикла команд. Пусть рабочий цикл процессора состоит из К этапов. Тогда при последовательном выполнении этапов продолжительность всех процедур рабочего цикла команды равна:

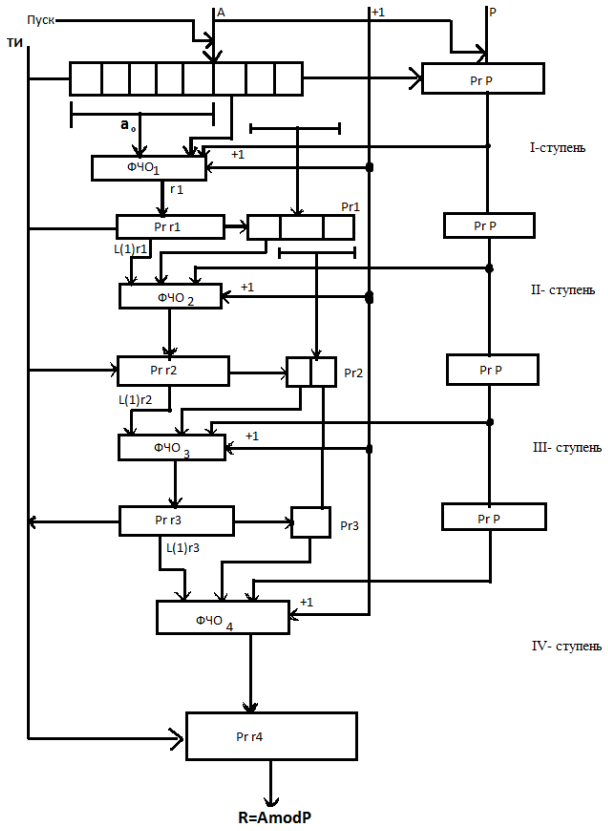

Рисунок 3.4 – Схема VI-ступенчатого конвейера

Результаты, вычисленные на i-й ступени на формирователе частичных остатков ФЧОi, передаются для дальнейшей обработки в (i+1) ступень конвейера. Перенос информации со ступени на ступень происходит через буферные регистры (БРгi), размещенные между ними. Выполнившая свою операцию i-я ступень помещает результат в i-й буферный регистр и может приступить к обработке следующей порции данных, в то время как очередная (i+1) ступень конвейера в качестве исходных использует данные, хранящиеся в i-м буферном регистре, расположенном на ее входе. Синхронность работы конвейера обеспечивается тактовыми импульсами (ТИ), период которых определяется самый медленной ступенью конвейера и задержкой в триггерах буферного регистра. В конвейерном устройстве приведения по модулю, имеющем К ступеней, входные данные могут подаваться на вход с частотой в К раз большей, чем в случае обычного делительного устройства. С этой же частотой будет появляться и результат на выходе устройства

Вывод

Для достижения цели дипломной были решены следующие задачи:

1) Описаны теоретические основы шифрования данных в аспекте обеспечения информационной безопасности.

Решение данной задачи позволило сформулировать следующие выводы:

Под информационной безопасностью будет пониматься состояние защищенности информации и информационной среды от случайных или

преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, (в том числе владельцам и пользователям информации). Исходя из данного определения, можно констатировать, что защита информации – комплекс мероприятий, направленных на обеспечение информационной безопасности.

Основным инструментом защиты информации на данный момент является шифрование или криптографическая защита.

Криптографическая система – система обеспечения безопасности информации криптографическими методами, включает совокупность систем шифрования, расшифрования, генерации и распределения ключей и других подсистем, необходимых для реализации криптографических протоколов. Иногда криптографическую систему называют синонимом алгоритма или шифра.

2) Реализован сравнительный анализ методов и алгоритмов шифрования.

Решение данной задачи позволило сформулировать следующие выводы:

При сравнительном анализе алгоритмов шифрования необходимо учитывать следующие характеристики:

– практическую стойкость шифра;

– ресурсоемкость и энергоемкость;

– скорость работы.

Алгоритмы шифрования построены таким образом, что для вскрытия требуется перебор по ключевому пространству, поэтому стойкость шифра определяется длиной ключа.

Анализ существующих методов приведения чисел по модулю показал, что с точки зрения сложности аппаратной реализации и по быстродействию эффективным является построение устройства приведения чисел на базе делительных устройств. Они могут быть реализованы по алгоритму деления с восстановлением и без восстановления остатка.

3) Описана реализация устройства приведения чисел по модулю на делителе с блокировкой отрицательных остатков.

Решение данной задачи позволило сформулировать следующие выводы:

Существует большое количество разнообразных методов формирования остатков при делении на модуль.

Разработанные на основе нового алгоритма деления с блокировкой отрицательного остатка схемы устройств приведения чисел по модулю на базе делителя с блокировкой отрицательных остатков, а также матричная и конвейеризированная схемы приведения по модулю в дальнейшем будут использованы при построении аппаратных устройств для криптографической защиты информации.

4 Технико-экономическое обоснование

Моя дипломная работа подразумевает проектирование схемы устройства умножения по модулю для быстродействующего выполнения операций приведения чисел по модулю, что обеспечивает более быстрое шифрование информации. При проектировании аппаратных и программно-аппаратных криптосистем с открытым ключом актуальным становится задача разработки эффективных схем для реализации одной из базовой операции – приведения числа по модулю. Для проектирования устройства понадобится контроллер, содержащий счетчик тактовых сигналов, формирователь частичного остатка, блок схемы ИЛИ, и регистры.

В данной части дипломной работы будут рассчитаны все расходы на разработку, требуемых материалов и устройств, затраты на программные обеспечения, затраты на электроэнергию и рабочий труд, а также амортизацию основного оборудования.

4.1 Расчет трудоемкости разработки программного продукта

Приведен перечень основных этапов и работ, которые нужно выполнить для точного определения трудоемкости разработки программного обеспечения. Трудоемкость работы определялась согласно нормам времени на проведение расчетов, анализа и исследований. Форма разделения работ по этапам с указанием трудоемкости их выполнения приведена в таблице 6.1.

Таблица 4.1 - Распределение работ по этапам и оценка их трудоемкости

Этапы разработки ПО	Вид работы	Трудоемкость, чел. час.
Этап 1	Постановка задач	15
Этап 2	Разработка и утверждение технического задания на разработку ПП	15
Этап 3	Поиск и изучение подобных программ и устройств	15
Этап 4	Поиск и изучение сопутствующей литературы	20
Этап 5	Составление аналитических графиков ПО	18
Этап 5	Выбор среды разработки программного обеспечения	14
Этап 6	Отладка программного обеспечения	24

Продолжение таблицы 4.1

Этап 7	Пробная реализация проекта	30
Этап 8	Оформление отчета и составление выводов о проделанной работе	20
Этап 9	Тестирование проекта	30
Этап 10	Внедрение проекта	20
Итого: трудоемкость выполнения программного проекта		221

Продолжительность рабочего дня равно 8 часам. То есть количество дней, затраченных на осуществление цели – 27 рабочих дней.

4.2 Расчет затрат на разработку программного продукта

Определение затрат на разработку программного продукта производится на основе существующей сметы, которая включает следующие статьи:

– материальные затраты;
– затраты на оплату труда;
– социальный налог;
– амортизация основных фондов;

Статья «Материальные затраты» состоит из основных и вспомогательных материалов, энергии, которые необходимы для разработки программного продукта. Расчет затрат на материальные ресурсы производится по форме, приведенной в таблице 4.2.

Таблица 4.2 – Затраты на материальные ресурсы

Наименование материала	Марка	Ед. измерения	Количество	Цена за ед. в тенге	Сумма в тенге
Офисная бумага, А4	Белоснежка	Пачка	2	1500	3000
Наименование материала	Марка	Ед. измерения	Количество	Цена за ед. в тенге	Сумма в тенге
Тетрадь А4 (96 листов)	Magister	Штук	1	250	250
Блокнот (96 листов)	OFFICE	Штук	1	650	650
Ручка	Rotomac	Штук	5	120	600

Продолжение таблицы 4.2

Карандаш	Hatber «PERFECT»	Штук	5	65	325
Компьютерная мышь (беспроводная)	HP Classic mouse	Штук	1	7990	7990
Итого					12815

При покупке нового ноутбука Acer A71 в нем предусмотрены встроенная операционная система и дополнительное программное обеспечение, поэтому затраты на покупку новой операционной системы Windows 8.1 и лицензионную MS Office производиться не будут.

Таблица 4.3 – Затраты на ОС и ПО, необходимые для проекта

Наименование материала	Марка	Ед. измерения	Количество	Цена за ед. в тенге	Сумма в тенге
Ноутбук	Acer A71	Шт.	1	190000	190000
Принтер	Samsung M2070	Шт.	1	48500	48500
Модем	TP-Link TL-WR740N	Шт.	1	8900	8900
ОС	Windows 10	Шт.	1	-	-
ПО	MS Office	Шт.	1	-	-
	Embarcadero® RAD Studio XE8	Шт.	1	-	-
Итого					247400

Общая сумма затрат на материальные ресурсы ($З_м$) определяется по формуле:

$$З_м = \sum P_i \times Ц_i, \quad (4.1)$$

где P_i– расход i-го вида материального ресурса, натуральные единицы;
$Ц_i$– цена за единицу i-го вида материального ресурса, тг;
i – вид материального ресурса;
n – количество видов материальных ресурсов.

$З_м = 12815 + 247400 = 260\ 215$ (тг)

Материальные затраты на программный проект составят 260 215 тенге. Все материальные затраты лягут на основные средства

4.3 Расчет затрат на электроэнергию

Очень важно рассчитывать затраты на электроэнергию, потому как в во время работы используется электрооборудование. Время работы оборудования для разработки программного продукта берется равным 224 часов для ноутбуков и модема, данное количество часов было рассчитано в таблице 6.1. Для принтера время работы для разработки программного продукта берется равным 12 часов, так нет необходимости постоянного его использования.

$$Э = З_{эл.эн.обор} + З_{доп.нуж}, \quad (4.2)$$

где $З_{эл.эн.обор}$ – затраты на электроэнергию оборудования;
$З_{доп.нуж.}$ – затраты электроэнергии на дополнительные нужды.

Расходы электроэнергии на оборудование рассчитывается по формуле:

$$З_{эл.эн.обор} = \sum W \times К_{исп} \times S \times T, \quad (4.3)$$

гдеW – потребляемая мощность, Вт;
$К_{исп}$ – коэффициент использования ($К_{исп}$ = 0,7-0,9);
T – время работы;
S – тариф (1кВт/ч = 18,65 тг).

Сводные результаты расчета затрат на электроэнергию представлены в таблице 6.4.

Таблица 4.4 – Затраты на электроэнергию

Наименование приборов	Паспортная мощность, кВт	Коэффициент мощности	Время работы оборудования, ч	Цена ЭЭ тг/ кВтч	Сумма, тг
Ноутбук	0,6	0,7	221	18,65	1731,093
Модем	0,08	0,9	100	18,65	134,28
Принтер	0,5	0,9	12	18,65	100,71
Кондиционер	0,8	0,9	200	18,65	2685,6
Освещение	0,3	0,7	221	18,65	865,54
Итого					5 517,22

$З_{эл.эн.обор}$ = 5 517,22 (тенге)

Затраты на дополнительные потребности берутся по укрупненному показателю в размере 5% от затрат на оборудование:

$$З_{доп.нуж} = 5\% \times З_{эл.эн.обор} \quad (4.4)$$

Затраты на дополнительные потребности рассчитаны по формуле (4.4):

$З_{доп.нуж}$ = 0,05 × 5 517,22= 275,861 (тенге)

Таким образом суммарные затраты на электроэнергию составляют:

Э = 5 517,22+ 275,861= 5793,081 (тенге)

4.4 Расчет затрат на оплату труда

Над разработкой проекта работают два сотрудника:

- руководитель проекта – изучает предметную область, проводит анализ требований к системе, занимается внедрением и поддержкой;
- разработчик – создает и реализует модель, занимается тестированием и отладкой программного продукта;

Общая сумма затрат на оплату труда ($З_{тр}$) определяется по формуле:

$$З_{тр}=\sum ЧС_i \times Т_i \quad (4.5)$$

где $ЧС_i$– часовая ставка i-го работника, тг;

Ti – трудоемкость разработки модели, чел.×ч;

i – категория работника;

n – количество работников, занятых разработкой ПП.

На этапах разработки, участники разработки задействованы неравноценно, для этого необходимо рассчитать часовую ставку работника, а затем общий размер заработной платы.

Часовая ставка работника может быть рассчитана по формуле:

$$ЧС_i=\frac{ЗПi}{ФРВi} \quad (4.6)$$

где Зпi – месячная заработная плата i-го работника, тг;

ФРВi- месячный фонд рабочего времени i-го работника, час

Месячная заработная плата сотрудников:

Руководитель проекта – 180 000 тг;

Разработчик – 120 000 тг.

$ЧС_i$= 180 000 / 22 × 8 = 1 022,72 тг/ч

$ЧС_i$= 120 000 / 22 × 8 = 681,81 тг/ч

Часовая ставка руководителя проекта составляет 1 022,72 (тг/ч), трудоемкость разработки – 90 ч. Часовая ставка разработчика составляет 681,81 (тг/ч), трудоемкость разработки – 216 ч.

Рассчитаем общую сумму затрат на оплату труда по формуле (4.5):

$З_{тр}$ = 1 022,72 × 90 + 681,81 × 216 = 239 315,76 (тенге)

Сводные результаты расчета затрат на оплату труда показаны в таблице 4.5

Таблица 4.5 – Расчёт основной заработной платы разработчиков

Категория работника	Квалификация	Трудоемкость разработки ПП, час.	Часовая ставка, тг/ч	Сумма, тг.
Руководитель проекта	Инженер	90	1 022,72	92 044,8
Разработчик	Программист	216	681,81	147270,96
Итого				239 315,76

4.5 Расчет затрат по социальному налогу

Социальный налог – согласно Налоговому кодексу Республики Казахстан составляет 9,5 % от ФОТ (фонда оплаты труда). Следует отметить, что пенсионные отчисления не облагаются социальным налогом.

$$С_н = (ФОТ- ПО)\times 0,095 \quad (4.7)$$

где ПО - отчисления в пенсионный фонд, 10% от ФОТ.

Социальный налог рассчитываем по формуле (4.7):

ПО = 239 315,76× 0,1 = 23 931,576 тенге;
$С_н$ = (239 315,76 – 23 931,576) × 0,095 = 20 461,49 тенге

Сводные результаты расчета затрат представлены в таблице 4.7.

Таблица 4.7 - Начисление социального налога

Категория работника	Количество человек	Заработная плата, тг	Пенсионные отчисления, тг	Социальный налог, тг
Руководитель проекта	1	92 044,8	9 204,48	7 869,75
Разработчик	1	147270,96	14 727,09	12591,66
Итого				20 461,49

4.6 Амортизация основных фондов и прочие затраты

Годовые нормы амортизации ОФ принимаются по налоговому кодексу РК или определяются, исходя из возможного срока полезного использования ОФ. Амортизация основных фондов определяется:

$$А_г = \frac{С_{об}\times Н_а}{100} \quad (4.8)$$

где, $С_{об}$ – стоимость оборудования;
$Н_а$ – норма амортизации (норма амортизация = 20);

По формуле 5.8 рассчитаем сумму амортизационных отчислений за год для ноутбука:

$$A_г = \frac{190000 \times 20}{100} = 38\,000 \text{ тг}$$

Рассчитаем сумму амортизации за время разработки:

$$A_р = \frac{28\,000 \times 28}{365} = 2\,915 \text{ тг}$$

Аналогичным способом рассчитаем сумму амортизации для остального оборудования.

Результаты расчетов приведены в таблице 6.6

Таблица 4.8 - Амортизация основных фондов

Наименование оборудования и ПО	Стоимость оборудования и ПО, тг	Годовая норма амортизации, %	Сумма амортизации за год, тг	Сумма амортизации за время разработки, тг
Ноутбук	190 000	20	38 000	2 915
Принтер	48500	20	9700	744,1
Модем	8900	15	1355	102,4
RAD Studio XE8	0	0	0	0
ИТОГО амортизация основных средств			49055	3761,5

Смета затрат на разработку программного продукта

На основании полученных данных по отдельным статьям составляется смета затрат на разработку программного продукта по форме, приведенной в таблице.

Таблица 4.9 – Смета затрат на разработку программного продукта

Статьи затрат	Сумма, тг
Затраты на оборудование	247400
Затраты на программное обеспечение	0
Затраты на оплату труда	239 315,76
Социальные налоги	20 461,49
Затраты на электроэнергию	5 517,22
Амортизация основных фондов	3 052,56
Прочие расходы (интернет)	22 404
Итого по смете	538 151,03

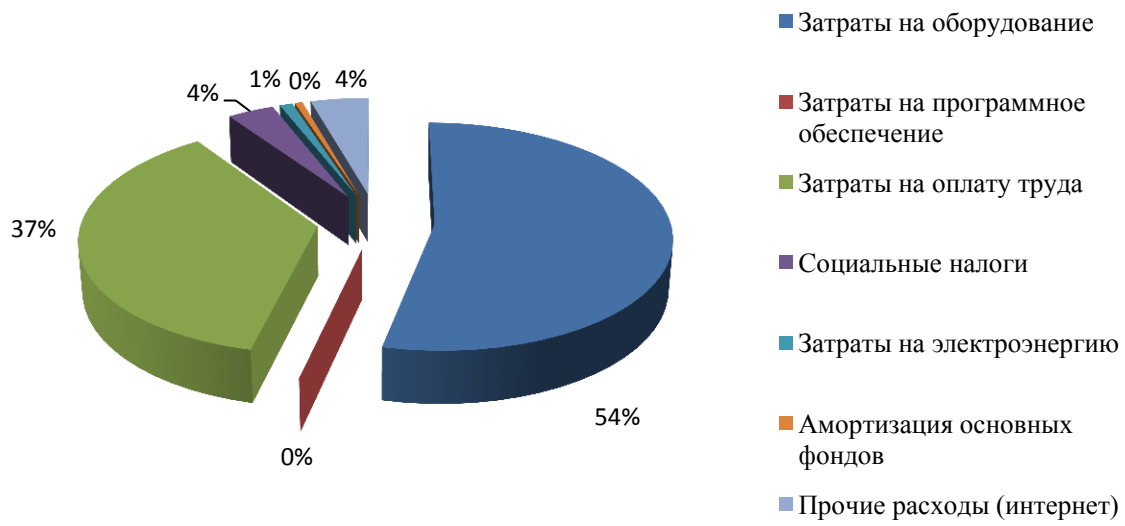

Рисунок 4.1 - Диаграмма структуры эксплуатационных затрат

4.7 Определение возможной цены программного продукта

Величина возможной (договорной) цены программного продукта устанавливается на основе эффективности, качества и сроков её выполнения на уровне, отвечающем экономическим интересам заказчика (потребителя) и исполнителя.

Договорная цена ЦД для прикладных программных продуктов рассчитывается по формуле:

$$Ц_Д = З_{НИР}\left(1 + \frac{Р}{100}\right) \quad (4.9)$$

где $З_{НИР}$- затраты на разработку ПП, тг;

Р – средний уровень рентабельности ПП. % (принимается в размере 20%).

$Ц_Д$ = 538 151,03× (1 + 20/100) = 645 781,23 тенге

Рентабельность - 107630,20

Далее определяется цена реализации с учетом налога на добавленную стоимость (НДС), ставка (НДС) устанавливается законодательно. Налоговым Кодексом РК. На 2019 год ставка НДС установлена в размере 12%.

Цена реализации с учетом НДС рассчитывается по формуле:

$$Ц_р = Ц_Д + Ц_Д \times НДС \quad (4.10)$$

645 781,23 + 645 781,23× 0,12 = 646 389,75 + 77 566 =
= 723 274,98432≈ 730 000,00 тенге

Рассчитанную возможную цену ПП можно округлить до 730 000,00 тенге.

Вывод

Данная глава дипломного проекта содержит экономические расчеты, которые позволяют определить затраты необходимые для разработки программного продукта. Расчеты включают в себя:

- расчет трудоемкости разработки программного продукта;
- расчет материальных затрат на разработку программного продукта;
- расчет материальных затрат на электроэнергию;
- расчет материальных затрат на оплату труда;
- расчет материальных затрат на социальный налог;
- амортизация основных фондов и прочие затраты.

Для потребителя основным показателем будет считаться оптимальная цена программного продукта и его производительность. Цена и полезность программного продукта должна обладать равновесием, чтобы покупатель был заинтересован в приобретении разработки. Качественным результатом для покупателя считается, что приобретенное программное обеспечение полностью покрывает все необходимые задачи, которые встают перед потребителем. Так же в последней главе был произведен расчет договорной цены программного продукта, который равняется 730 000,00 тенге, данная сумма является рациональной с точки зрения экономической эффективности.

Затраты на разработку ПО составили 538 151 тг. Договорная цена составляет 730 000,00. Итоговая прибыть 107 630,00 тг.

5. Безопасность жизнедеятельности

5.1 Анализ условий труда

В данной дипломной работе я разрабатываю аппаратный метод шифрования. Для его разработки требуется небольшое закрытое помещение, для 5 человек, сотрудник службы безопасности и несколько разработчиков имеющие навыки в области шифрования, криптографии и знания ЭВМ. В помещении есть 5 рабочих мест со стационарными компьютерами модели Asus ROG которые работают достаточно тихо и не вызывают шума, и так же аппаратными устройствами шифрования. Помещение площадью 280 м2 длиной 10 метров шириной 7 метров и высотой 4 метра очень хорошо освещаемо благодаря источнику освещения люминесцентных ламп, мощностью 50 Вт/м2 и остеклению площадью 24м2. Но в помещении полностью отсутствует система кондиционирования для благоприятной работы сотрудников, в следствии в разделе БЖД задаюсь целью рассчитать системы кондиционирования и подобрать соответствующую модель по основным характеристикам.

Ход работы:

1) рассчитать тепловые нагрузки в помещении: внутренние и наружные;

2) рассчитать количество воздуха, необходимое для подачи в помещение;

3) по найденному значению количества воздуха подобрать соответствующую модель кондиционера;

4) привести основные характеристики выбранного кондиционера;

5) привести схему расположения кондиционера в помещении и схему подачи воздуха.

Таблица 5.1 – Исходные данные

Город	Алматы;
Параметры помещения (Д х Ш х В), м	10 х 7 х 4;
Данные по оборудованию	кол-во 5 шт.;
Мощность Роб, кВт/ч	0,5;
КПД η	0,75;
Данные по ист. света	мощ. N ос. уст., Вт/м^2 = 50;
Вид ист. св.	люминиц. лампы;
Число сотрудников, из них	мужчины = 4, женщины = 1;
Окна	кол-во 4;
Площадь 1 окна, м^2	6;
Общая площадь остекления, м^2	24м^2 ;
Расположение	СЗ;
Вид	остекление в один-х метал. переплет, загрязнение умеренное;
Расчетное время суток, ч.	10-11;
Температура в помещении, ^{0}С	летом 23, зимой 21;

5.2 Расчёт тепловых нагрузок в помещении: внутренние и наружные.

В помещениях различного назначения возникают чаще всего тепловые нагрузки, исходящие снаружи помещения (наружные); и тепловые нагрузки, возникающие внутри зданий (внутренние).

Наружные тепловые нагрузки.

Данные нагрузки представлены следующими составляющими:

– теплопоступления или теплопотери в результате разности температур снаружи и внутри здания через стены, потолки, полы, окна и двери.

– разность температур снаружи здания и внутри него летом является положительной, в результате чего имеет место приток тепла снаружи во внутрь помещения; и наоборот – зимой эта разность отрицательна и направление потока тепла меняется;

– теплопоступления от солнечного излучения через застекленные площади; данная нагрузка проявляется в форме ощущаемого тепла;

– теплопоступления от инфильтрации.

В зависимости от времени года и времени суток наружные тепловые нагрузки могут быть положительными. Теплопоступления и теплопотери в результате разности температур определяются по формуле 5.1:

$$Q_{огр}=V_{пом}*X_0*(t_{Нрасч}-t_{Врасч}),\ Вт \qquad (5.1)$$

где $V_{пом.}$ – объем помещения, $м^3$: $V_{пом}= 10\cdot17\cdot4=680\ м^3$; $X_о$ – удельная тепловая характеристика, $Вт/м^3\ ^0C$: $X_0=0.42\ Вт/м^3\ ^0C$;

$t_{Нрасч}$ – наружная температура (параметр А). Для холодного периода – средняя температура самого холодного месяца в 13 часов, для теплого периода – средней температуре самого жаркого месяца в 13 часов.

$t_{Врасч}$ – внутренняя температура, выбирается с учетом комфортных условий или технологических требований, предъявляемых к производственным процессам.

Для теплого времени года:

$$t_{Нрасч} = 31\ ^0C$$
$$t_{Врасч} = 24\ ^0C$$
$$Q_{огр.}= 680\cdot0,42\cdot7=1999,2\ Вт$$

Для холодного времени года

$$t_{Нрасч} = -14\ ^0C$$
$$t_{Врасч} = 21\ ^0C$$
$$Q_{огр.}= 680\cdot0,42\cdot35 = 9996\ Вт$$

Избыточная теплота солнечного излучения в зависимости от типа стекла почти до 90% поглощается средой помещения, остальная часть отражается. Максимальная тепловая нагрузка достигается при максимальном уровне излучения, которое имеет прямую и рассеянную составляющие.

Интенсивность излучения зависит от ширины местности, времени года и времени суток.

Теплопоступление от солнечного излучения через остекление определяется по формуле 5.2:

$$Q_р=(q^I F_0{}^{II} + q^{II} F_0{}^{II}) * \beta_{с.з.} \quad (5.2)$$

где q^I, q^{II} – тепловые потоки от прямой и рассеянной солнечной радиации, Вт/м^2 ;

$F^I_о$, $F^{II}_о$ – площади светового проема, облучаемые и необлучаемые прямой солнечной радиацией, м^3;

βс. з. – коэффициент теплопропускания. βс. з. = 0.15

При отсутствии наружных затеняющих козырьков, ребер и т. д. для периода облучения остекления солнцем, когда его лучи проникают через окно в помещение $F^I_о = F_о$; $F^{II}_о = 0$, (5.3):

$$Q_р=q^I F_0 * \beta_{с.з.} = (q_{вп}+q_{вр}) * K_1{}^c * K_2 * \beta_{с.з.} * n * S_0, \text{ Вт} \quad (5.3)$$

где $Q_{вп}$; $q_{вр}$ – тепловые потоки от прямой рассеянной радиации, Вт/м^2.

По таблице 5 [1] для широты в 440 СШ до полудня в 11-12 ч. при расположении З:

$Q_{вп}$ = 69 Вт/м^2 ; $q_{вр}$ = 74 Вт/м^2 ;

$F_о = nS_о = 4 \cdot 6 = 24$ м^2 – площадь светового проема (n – число окон; $S_о$ – площадь 1 окна);

K_1 – коэффициент затемнения остекления переплетами (K^C_1 – для облученных проемов):

$K^C_1 = 0.72$;

K_2 – коэффициент загрязнения остекления:

$K_2 = 0.9$.

Тогда:

$Q_р$=(69+74)*0,72*0,9*0,15*4,5=62,54 Вт.

Для широты в 440 СШ до полудня в 11-12 ч. при расположении В:

$Q_{вп}$ = 211 Вт/м^2; $q_{вр}$ = 89 Вт/м^2 ;

$F_о = nS_о = 4 \cdot 72 = 24$ м^2 – площадь светового проема (n – число окон; $S_о$ – площадь 1 окна);

Тогда:

$Q_р$=(211+89)*0,72*0,9*0,15*4,5=131,22 Вт.

Тогда общее теплопоступление солнечного излучения с обеих окон равно:

$Q_р$=62,54+131,22=193,76 Вт.

Внутренние тепловые нагрузки.

Внутренние нагрузки в жилых, офисных или относящихся к сфере обслуживания помещениях слагаются в основном из тепла:

– выделяемого людьми;

– выделяемого лампами и осветительными, электробытовыми приборами;

– выделяемого компьютерами, печатающими устройствами фотокопировальными машинами пр.

В производственных и технологических помещениях различного назначения дополнительными источниками тепловыделений могут быть: нагретое производственное оборудование, горячие материалы, в том числе жидкости и различного рода полуфабрикаты, продукты сгорания и химических реакций.

Теплопоступления от людей зависит от интенсивности выполняемой работы и параметров окружающего воздуха. Тепло, выделяемое человеком, складывается из ощутимого (явного), то есть передаваемого в воздух помещения путем конвекции и лучеиспусканий, и скрытого тепла, затрачиваемого на испарение влаги с поверхности кожи и из легких.

По таблице 8 [1] летом при 24 ^{0}С один мужчина выделяет явного тепла 61 Вт, а общего – 102 Вт. Женщина выделяет 85% от нормы тепловыделений взрослого мужчины. Тогда выделение явного тепла в помещении составит:

$Q_л^я = 61*4+61*1*0,85=295,85$ Вт.

А выделение общего тепла:

$Q_л^о = 102*4+102*1*0,85=494,7$ Вт.

По таблице 8 зимой при 20 ^{0} С один мужчина выделяет явного тепла 82 Вт, а общего – 103 Вт. Женщина выделяет 85% от нормы тепловыделений взрослого мужчины. Тогда выделение явного тепла в помещении составит:

$Q_л^я = 82*4+82*1*0,85=397,7$ Вт.

А выделение общего тепла:

$Q_л^о=103*4+103*1*0,85=499,55$ Вт.

Теплопоступление от осветительных приборов, оргтехники и оборудования рассчитывается следующим образом. Теплопоступление от ламп определяется по формуле (5.4):

$$Q_{осв}= \eta * N_{осв} * F_{пол} \quad (5.4)$$

где η – коэффициент перехода электрической энергии в тепловую (для люминесцентных ламп η=0.5-0.6);

$N_{осв}$ – установленная мощность ламп (N=50 Вт/м^2);

$F_{пол}$ – площадь пола:

$F_{пол}=17\cdot11=70$

Тогда:

$Q_{осв}=0,5\cdot50\cdot70= 1750$ Вт

Тепло, выделяемое производственным оборудованием, определяется по формуле (5.5):

$$Q_{об} = N_{уст} * K \quad (5.5)$$

$Q_{об}=1,8*10^3*5*0,95=8550$ Вт.

Теплопритоки, возникающие за счет находящейся оргтехники, – это 30% мощности оборудования:

$Q_{орг}$ = 1,8*10^3*5*0,3=2700 Вт.

5.3 Расчёт количества воздуха, необходимое для подачи в помещение.

На основании выполненных расчетов составим баланс теплопоступлений в помещении:

Лето: $Q_{изб}$=295,85+686,25+1750+8550+2700+1999,2 = 15981, Вт

Зима: $Q_{изб}$=295,85+686,25+1750+8550+2700 +9986 =23968, Вт

Так как тепловой баланс для лета больше зимнего теплового баланса, то рассчитаем тепло напряжённость воздуха по формуле:

$$Q_н = \frac{Q_{изб.лето} \times 860}{V_{пом}}$$

$$Q_н = \frac{23968 \cdot 860}{680} = 30312{,}4 \text{ ккал/м3}$$

При $Q_н$ >20ккал/м3 , Δt = 8 °С.

Определение количества воздуха, необходимое для поступления в помещение:

$$L = \frac{Q_{изб} \times 860}{C \times \Delta t \times \gamma}$$

$$L = \frac{23968 \cdot 860}{0{,}24 \cdot 8 \cdot 1{,}206 \cdot 10^4} = 890{,}8 \text{ м3/час}$$, где

С=0,24 ккал/(кг°С) – теплоемкость воздуха,

γ=1,206 кг/$м^3$ – удельная масса приточного воздуха.

Определение кратности воздухообмена:

$$N = \frac{593{,}5}{680} = 1.31 \text{ час}^{-1}$$

5.4 По найденному значению количества воздуха подбираем соответствующую модель кондиционера.

Исходя из полученных данных, выберем кондиционер сплит-системы настенного типа.

Таблица 5.2 – Основные технические характеристики настенного кондиционера серии TOSHIBA RAV-SM1102CT-E

Эл. питание В/Гн	Произв. по холоду, кВт	Потр. эл мощн, кВт	Потребл ток, А	Произв. по теплу, кВт	Размер (внешн. блок) мм	Расход воздуха, м3/ч	Размер (внутр. блок) мм
220/50/1	14,07	7300	10,2	7330	L 845 H 700	8000	L 735 H 620

					В 320		В 310

5.5 Приводим схему расположения кондиционера в помещении и схему подачи воздуха.

Во внешнем блоке находятся компрессор, конденсатор и вентилятор. Внешний блок можно установить на стене здания, на крыше или на черда-ке, в подсобном помещении или на балконе, то есть в таком месте, где го-рячий конденсатор может продуваться атмосферным воздухом более низ-кой температуры. Внутренний блок устанавливается непосредственно в кондиционируемом помещении и предназначен для охлаждения или нагревания воздуха, фильтрации его и создания необходимой подвижно-сти воздуха в помещении. Внутренние блоки поддерживают заданную температуру, обеспечивают равномерное распределение воздуха в поме-щении и работает почти без шума (уровень шума 37-41 дБ).

Настенным кондиционером можно управлять с помощью пульта ди-станционно, он позволяет задать разные режимы работы, например функ-ция обогрева или наоборот охлаждения, вентилиции помещения, так же присутствует ночной режим. Можно также задать нужную температуру, он будет его поддерживать перманентно. Есть возможность выбрать ре-жим вентяляции, к нему подобрать таймер, он будет работать в установ-ленный промежуток времени. Регулируется также и направление потока воздуха.

Поскольку в помещение необходимое количество воздуха является 890,8 м3/час, стоит использовать два кондиционера с разными количества-ми растраты воздуха и поэтому они вместе смогут компенсировать его не-обходимое количество

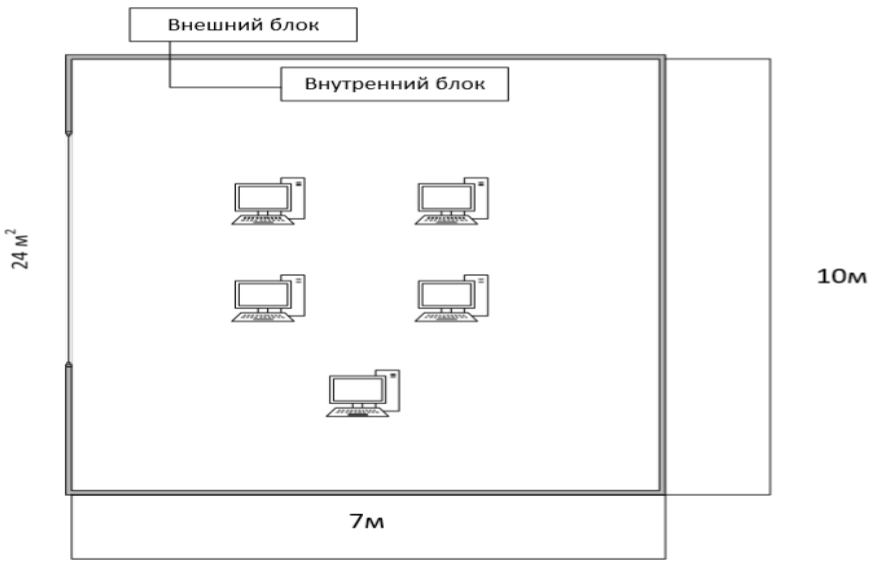

Рисунок 5.1 – Схема расположения кондиционера в производственном помещении

Вывод

В этой главе были рассчитаны тепловые нагрузки в помещении, внешние и внутренние. Согласно расчетам, была выбрана модель кондиционера с подходящими характеристиками. Из расчетов видно, что при достаточно малом пространстве и среднем количестве людей и оборудования количество избыточного тепла велико, что подразумевает установку достаточно мощной системы кондиционирования воздуха.

Обеспечение комфорта воздуха в жилых и производственных помещениях зависит от систем аспирации, вентиляции, отопления и кондиционирования воздуха.

Задача кондиционирования воздуха заключается в выполнении вентиляции и обогрева, а также в поддержании таких параметров воздушной среды, в которых каждый человек будет чувствовать себя комфортно со своей индивидуальной системой автоматической терморегуляции, не замечая влияния этой среды. В результате был произведен расчет кондиционирования помещения и выбора типа и типа кондиционера для этой комнаты.

Список литературы

1 Адаменко М.В. Основы классической криптологии. Секреты шифров и кодов. - М.: ДМК Пресс, 2017. - 256 с.

2 Алгоритмические основы эллиптической криптографии / А. А. Болотов [и др.]. – М.: Изд-во РГСУ, 2018. – 499 с.

3 Алферов А.П., Зубов А.Ю., Кузьмин А.С., Черемушкин А.В. Основы криптографии. – М.: Гелиос АРВ. – 2018. – 480 с.

4 Анисимов В.В. Криптография: метод. указания. – Хабаровск: Изд-во ДВГУПС, 2018. – 32 с.

5 Арсентьев М.В. К вопросу о понятии «информационная безопасность» // Информационное общество. - 2018. - № 4-6. – С. 18-23

6 Бабаш А.В., Баранова Е.К. Оперативные методы криптографии. - М.: РГСУ, 2017. - 104 с.

7 Бабаш А.В., Шанкин Г.П. Криптография. - М.: СОЛОН-ПРЕСС, 2018. - 512 с.

8 Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. - М.: Горячая Линия - Телеком, 2019. - 176 с.

9 Болелов Э.А. Криптографические методы защиты информации. Часть I. Симметричные криптосистемы. - М.: МГТУ ГА, 2019. – 80 с.

10 Болотов А.А., Гашков С.Б., Фролов А.Б. Элементарное введение в эллиптическую криптографию. Протоколы криптографии на эллиптических кривых. - М.: КомКнига, 2018. - 306 с.

11 Василенко О.Н. Теоретико-числовые алгоритмы в криптографии. – М.: МЦНМО, 2019. – 328 с.

12 Введение в криптографию / под ред. В. В. Ященко. – СПб.: Питер, 2017. – 288 с.

13 Вихорев С. Как определить источники угроз / С. Вихорев, Р.Кобцев // Открытые системы. - 2019. - №07-08. - С. 43.

14 Волчков А. Современная криптография / А.Волчков // Открытые системы.- 2019. - №07-08. - С. 48.

15 Герасименко В.А. Защита информации в автоматизированных системах обработки данных. - М.: Энергоатомиздат, 2017. – 256 с.

16 Гмурман А.И. Информационная безопасность. - М.: БИТ-М, 2017. - 387 с.

17 Касто В.Д. Просто криптография. - М.: Страта, 2017. - 208 с.

18 Коробейников А.Г. Математические основы криптологии. – СПб.: СПбГУ ИТМО, 2018. – 106 с.

19 Коутинхо С. Теория чисел. Алгоритм RSA. – М.: Постмаркет, 2017. – 328 с.

20 И. Ф. Мазалов, К. Г. Мустафин, Е. М. Тыщенко, М. А. Сералиева Методические указания по выполнению РГР для студентов специальности 5В0731100-БЖ. – Алматы: АУЭС, 2015. – 38 с.