МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Физико-технический факультет**

**Кафедра теоретической физики и**

**компьютерных технологий**

**КУРСОВОЙ ПРОЕКТ**

**ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ЭЛЕКТРОННОГО ДОКУМЕТООБОРОТА**

Работу выполнил \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Мустафин Оскар Искандерович

Курс 2

Направление 09.03.02 Информационные системы и технологии

Научный руководитель

преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Т.В. Арутюнян

Нормоконтролер инженер \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Г.Д.Цой

Краснодар 2018

СОДЕРЖАНИЕ

[ВВЕДЕНИЕ 3](#_Toc512283002)

[1 Электронный документооборот 4](#_Toc512283003)

[1.1 Понятие электронного документооборота 4](#_Toc512283004)

[1.2 Функции и эффективность ЭДО 6](#_Toc512283005)

[1.3 Системы электронного документооборота 7](#_Toc512283006)

[1.4 Виды СЭД 9](#_Toc512283007)

[1.5 Внедрение электронного документооборота 10](#_Toc512283008)

[2 Информационная безопасность ЭД 13](#_Toc512283009)

[2.1 Понятие информационной безопасности 13](#_Toc512283010)

[2.2 Аутентификация 15](#_Toc512283011)

[2.3 Защита документа 16](#_Toc512283012)

[2.4 Обеспечение безопасного доступа 16](#_Toc512283013)

[2.5 Разграничения прав пользователя 17](#_Toc512283014)

[2.6 Конфиденциальность 18](#_Toc512283015)

[3 Шифрование с открытым ключом. АЛГОРИТМ RSA 18](#_Toc512283016)

[3.1 Определение RSA 18](#_Toc512283017)

[3.2 Криптосистема с открытым ключом 18](#_Toc512283018)

[3.3 Описание алгоритма RSA 19](#_Toc512283019)

[3.3.1 Генерация ключей RSA 19](#_Toc512283020)

[3.3.2 Шифрование и расшифровывание в RSA 20](#_Toc512283021)

[3.4 Безопасность схемы RSA 21](#_Toc512283022)

[3.5 Пример шифрования RSA 22](#_Toc512283023)

[3.6 Условие работы алгоритма 23](#_Toc512283024)

[ЗАКЛЮЧЕНИЕ 25](#_Toc512283025)

[СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ 26](#_Toc512283026)

# ВВЕДЕНИЕ

В современном мире большую популярность приобрел электронный документооборот. Огромное количество информации, которая хранится в документах часто передается от одного человека к другому. Следовательно, изучение способов защиты этих данных просто необходима в современном мире. Основная проблема затрагиваемая в данной курсовой работе – это способы и методы повышения информационной безопасности внутри предприятий.

Основные задачи работы:

- Изучить и проанализировать литературу по данной тематике;

- Изучить основные понятия, касающиеся электронного документооборота, и информационной безопасности;

- Изучить влияния различных показателей на электронный документооборот. Выявить основные трудности возникающие при его защите;

- Рассмотреть один из методов шифрования.

Цель работы заключается в ознакомлении с электронным документооборотом , изучении способов его защиты и проблем связанных с этим.

### 1 Электронный документооборот

### 1.1 Понятие электронного документооборота

Электронный документооборот (ЭДО) — это система автоматизированных процессов обработки электронных документов, реализующая концепцию «безбумажного делопроизводства». Развитие и активное внедрение электронного документооборота началось в 90-е годы, когда на российском рынке появилось большое количество программ по автоматизации делопроизводства. С тех пор эта отрасль активно развивается. Все больше организаций стремятся внедрить у себя систему электронного документооборота, чтобы повысить эффективность использования рабочего времени и свести к минимуму затраты на ручную обработку документов.

Первые шаги по автоматизации отечественного делопроизводства были предприняты еще во времена СССР в аппарате ЦК КПСС. В то время функционал системы электронного документооборота был весьма невелик и представлял собой одно рабочее место секретаря, занимавшегося вводом в систему регистрационно-контрольных карточек, ведением журналов учета документов, составлением отчетов и поиском по регистрационным карточкам. Основным элементом электронного документооборота является электронный документ, создаваемый с помощью средств компьютерной обработки информации и хранящийся в виде файла того или иного формата на машинном носителе. Внедрение электронного документооборота позволяет предприятию получить следующие преимущества:

- однократная регистрация документа, позволяющая безошибочно идентифицировать его в системе;

- параллельное выполнение нескольких операций, сокращающее время движения документа и повышающее оперативность исполнения;

- непрерывное движение документа, дающее возможность выявить ответственного за его исполнение в любой момент процесса;

- единая база документов, исключающая возможность их дублирования;

- результативный поиск документа при наличии о нем минимальной информации;

- эффективная система отчетности, позволяющая контролировать движение документа на каждом этапе документооборота.

В зависимости от специфики деятельности организации выделяют несколько видов электронного документооборота:

- производственный ЭДО;

- управленческий ЭДО;

- архивное дело;

- кадровый ЭДО;

- бухгалтерский ЭДО;

- складской ЭДО;

- технологический ЭДО;

- секретный ЭДО;

- конфиденциальный ЭДО.

Систем электронного документооборота может быть столько же, сколько существует видов деятельности. При необходимости можно автоматизировать любой частный документооборот.

### 1.2 Функции и эффективность ЭДО

Набор необходимых функций ЭДО определяется задачами, стоящими перед автоматизацией документооборота в компании.

Базовые функции ЭДО:

- создание электронной версии документа;

- создание атрибутной карточки документа;

- формирование текста из готового шаблона с подстановкой в него значений переменных из карточки документа; поиск карточек документов;

- формирование электронного документа с использованием шаблона на бланке организации;

- сохранение документов в различных форматах;

- создание маршрутов документа и управление его движением;

- ведение журналов, классификаторов и справочников; регистрация и классификация документов, регистрируемых в программе;

- рассылка напоминаний и уведомлений; согласование документов;

- формирование отчетов о движении и исполнении документов.

Эффективность использования электронного документооборота в организациях оценивается количественно и качественно. Количественные показатели могут быть измерены и оценены с точки зрения материальных и временных затрат:

- сокращение времени в среднем на 75% на обработку и создание документов: регистрация, рассылка, поиск, выполнение контрольных операций;

- ускорение движения информационных потоков: передача документа от подразделения к подразделению или компании-партнеру, подготовка типовых документов, согласование, скорость распространения информации внутри компании;

- экономия материалов и ресурсов в виде сокращения расходов на канцелярские принадлежности, расходные материалы и хранение документов.

Качественные показатели оцениваются с точки зрения улучшения и развития нескольких аспектов деятельности компании:

* рост производительности труда работников до 25%, благодаря наличию единого информационного пространства, упрощению процессов коллективной работы, эффективному контролю над исполнением документов;
* снижение рисков потери документов;
* увеличение скорости согласования и утверждения документов;
* повышение корпоративной культуры.

Как показывает практика, экономический эффект от внедрения системы электронного документооборота на предприятии будет тем больше, чем больше сотрудников будут вовлечены в ЭДО.

### 1.3 Системы электронного документооборота

Система электронного документооборота (СЭД) — это специальное приложение, обеспечивающее участникам обмен электронными документами, имеющими юридическую значимость. Внедрение системы электронного документооборота (СЭД), позволяет приобрести огромную гибкость в обработке и хранении информации и заставляет бюрократическую систему компании работать быстрее и с большей отдачей. По данным ряда аналитиков, производительность труда персонала при использовании СЭД увеличивается на 20-25%, а стоимость архивного хранения электронных документов на 80% ниже по сравнению со стоимостью хранения бумажных архивов.

Все системы электронного документооборота могут быть классифицированы по нескольким признакам:

- СЭД с развитыми системами хранения и поиска информации. Их второе название — электронные архивы;

- СЭД с развитыми системами маршрутизации, обеспечивающие движение документов по заданным маршрутам;

- СЭД с системой поддержки управления организацией и накопления знаний. Обычно эти системы сочетают в себе свойства двух предыдущих. При этом в такой системе возможно использование как жесткой, так и свободной маршрутизации. Подобные СЭД используются в крупных компаниях и государственных структурах;

- СЭД с поддержкой совместной работы сотрудников. Такие системы нацелены на организацию коллективной работы сотрудников даже в том случае, если они разделены территориально. Предоставляют возможность поиска информации, обсуждений и назначения встреч, включая реальные и виртуальные, а также сервисы хранения и публикации документов;

- СЭД с дополнительными сервисами: управление проектами, электронная почта, биллинг, сервис CRM;

Наиболее востребованными функциями СЭД являются:

- Хранение и поиск документов;

- Поддержка делопроизводства;

- Маршрутизация и контроль исполнения документов: составление маршрутов документов, поддержка действий во время маршрутов, уведомление сотрудников о поступлении нового документа, автоматический контроль сроков исполнения;

- Составление аналитических отчетов, таких как отчет о текущей занятости, о выполнении работ по документам и о просроченных поручениях;

- Обеспечение информационной безопасности, которое включает аутентификацию пользователей, поддержку электронной цифровой подписи, шифрование документов и писем, аудит работы в системе.

Помимо перечисленных свойств важным является обеспечение юридической значимости электронных документов. Юридическая значимость позволяет организации защитить свои интересы в спорных ситуациях – как при договорных отношениях, так и внутри самой компании.

### 1.4 Виды СЭД

Особенностью российского внутреннего электронного документооборота организации является его вертикальная направленность: документ, прежде чем попасть к исполнителю, должен пройти ряд согласований и утверждений у вышестоящего руководства. Кроме того, в отечественном делопроизводстве присутствуют такие неотъемлемые части, как регистрационная система, подготовка отчетов, контроль исполнения. В связи с этим наиболее известными на российском рынке СЭД являются продукты местных разработчиков.

Поскольку разработчики предлагают множество программ автоматизации делопроизводства, важно не ошибиться при выборе той или иной СЭД. Существует несколько важных критериев, при помощи которых можно понять, подходит ли программа для компании или нет.

- Соответствие стандарту отрасли организации;

- Соответствие целям и задачам компании;

- Уровень технической поддержки СЭД со стороны компании-разработчика во время установки и в процессе эксплуатации;

- Возможность изменения СЭД в случае расширения деятельности организации;

- Доступность документации по администрированию или изменению настроек СЭД;

- Защита СЭД. Система должна обеспечивать защиту информации в соответствии с политикой безопасности компании;

- Время, необходимое на восстановление СЭД после сбоев в работе;

- Стоимость СЭД, которая включает стоимость покупки, лицензии, администрирования и технической поддержки;

Выбор системы зависит от того, что заказчик планирует от нее получить, какими ресурсами располагает и каков уровень развития компании в сфере организации электронного документооборота.

### 1.5 Внедрение электронного документооборота

Внедрение электронного документооборота в организации — не такая простая задача. Недостаточно просто приобрести программу, установить ее на компьютеры и запустить в работу. Успешность внедрения зависит от соблюдения нескольких условий:

- Активное участие в автоматизации делопроизводства со стороны руководства компании;

- Быстрое решение организационных вопросов, которые связанны с внедрением ЭДО, а также влияние на руководителей среднего звена и подчиненных, сопротивляющихся инновациям, помогает успешной реализации поставленной цели;

- Соблюдение этапов установки, что позволит выдержать необходимые сроки и уложиться в бюджет;

- Заинтересованность ключевых пользователей. При автоматизации документооборота необходимо учитывать интересы тех сотрудников, которые будут непосредственно работать в программе;

- Грамотная подготовка проектной документации позволит избежать разночтений у исполнителя и заказчика в процессе эксплуатации системы.

Не стоит пытаться подстроить все процессы документооборота предприятия под внедряемую систему, так же как и полностью переделывать систему под бизнес-процессы заказчика. Очень важно соблюсти золотую середину, применив передовые практики, уже имеющийся регламент работы компании и ее традиции. Чем больше в процессе внедрения учитываются перечисленные принципы, тем выше вероятность того, что переход предприятия на электронный документооборот будет удачным.

Порядок организации электронного документооборота в компании выглядит следующим образом:

1. Разработка технического задания;
2. Выбор IT-решения;
3. Описание бизнес-процессов;
4. Составление смет, графиков, списка необходимых ресурсов и общего плана работ;
5. Внедрение электронного документооборота;
6. Тестирование программы;
7. Запуск СЭД в эксплуатацию;
8. Контроль использования системы.

В процессе внедрения СЭД на предприятии неизбежно возникновение проблем и рисков, приводящих к нарушению сроков запуска проекта, превышению бюджета, неполному достижению целей, стоящих перед СЭД или даже к полному срыву внедрения программы. Специфика рисков при внедрении ЭДО, так же как и при внедрении любой информационной системы в масштабах всей организации обусловлена тем, что за относительно короткий срок необходимо перевести значительную часть сотрудников на новые и непривычные для них методы работы.

К основным рискам можно отнести следующие:

- консервативность сотрудников;

- недостаточная компьютерная грамотность работников;

- отсутствие регламентов на основные процессы;

- слабое техническое оснащение;

- отсутствие четкого управления проектом.

Чтобы предотвратить появление нежелательных проблем при организации электронного документооборота, необходимо детально спроектировать работу СЭД в компании, организовать ее поэтапное введение, обучить персонал и обеспечить ему оперативную поддержу в решении проблем, связанных с работой СЭД. В целом, внедрение электронного документооборота — это не просто инновация, но радикальный шаг к современному управлению информационными потоками.

### 2 Информационная безопасность ЭД

### 2.1 Понятие информационной безопасности

Информационная безопасность – это повышение безопасности работы с документами. В любой организации существует ряд проблем, связанных с безопасностью работы с бумажными и электронными документами. Основные классы таких проблем – это отсутствие разграничения доступа к документам и низкий уровень их сохранности. Безусловно, решение этих проблем требует системного подхода и должно осуществляться системными администраторами, службой безопасности и службой делопроизводства на разных уровнях – от физической защиты архивов бумажных документов и серверов до разработки и внедрения правил установки и использования грифов секретности. Внедрение системы электронного документооборота – важный шаг на пути обеспечения целостной системы безопасности работы с документами. От того, насколько полно в ней поддерживаются возможности обеспечения сохранности и конфиденциальности документов, во многом зависит общая безопасность документооборота предприятия.

Оценка уровня защищенности систем электронного документооборота. При построении системы защиты необходимо в первую очередь определить актуальные угрозы безопасности и возможность их предотвращения функциональными возможностями программного обеспечения системы, поскольку данная мера позволяет избежать значительных финансовых затрат и не допустить избыточности.

Самыми острыми проблемами при обеспечении информационной безопасности при использовании систем электронного документооборота являются:

- Угроза доступности – это программные сбои в работе системы; нарушение работы сети и средств вычислительной техники, в том числе вызванные атаками типа «отказ в обслуживании» и внедрением вредоносного ПО, стихийными бедствиями, отключение системы питания; блокирование или удаление информации, либо вследствие непреднамеренных действий пользователя;

- Угроза целостности – повреждение и уничтожение информации, искажение информации – как не намеренное в случае ошибок и сбоев, так и злоумышленное;

- Угроза конфиденциальности – это любое возможное нарушение конфиденциальности, в том числе кража, перехват информации, изменения маршрутов следования;

- Угроза работоспособности системы – всевозможные угрозы, реализация которых приведет к нарушению или прекращению работы системы; сюда входят как умышленные атаки, так и ошибки пользователей, а также сбои в оборудовании и программном обеспечении;

Защиту именно от этих угроз в той или иной мере должна реализовывать любая система электронного документооборота. При этом, с одной стороны, внедряя СЭД, упорядочивая и консолидируя информацию, увеличиваются риски реализации угроз, но с другой стороны, как это ни парадоксально, упорядочение документооборота позволяет выстроить более качественную систему защиты.

Основное проблемное место при организации защиты СЭД, как отмечают большинство разработчиков систем защиты, это не технические средства, а лояльность пользователей. Как только документ попадает к пользователю, конфиденциальность этого документа по отношению к пользователю уже нарушена. Техническими мерами в принципе невозможно предотвратить утечку документа через этого пользователя. Он найдет множество способов скопировать информацию, от сохранения его на внешний носитель до банального фотографирования документа с помощью камеры, встроенной в сотовый телефон. Основные средства защиты здесь – это организационные меры по ограничению доступа к конфиденциальным документам и работы с самим пользователем.

СЭД должна обеспечить сохранность документов от потери и порчи и иметь возможность их быстрого восстановления. 45% случаев потери информации приходится на физические причины (отказ аппаратуры, стихийные бедствия и подобное), 35% обусловлены ошибками пользователей и менее 20% – действием вредоносных программ и злоумышленников.

Безопасный доступ к данным внутри СЭД обеспечивается аутентификацией и разграничением прав пользователя.

### 2.2 Аутентификация

Обозначим процессы установления личности пользователя и процессы подтверждения легитимности пользователя на то или иное действие или информацию одним термином – аутентификацией, понимая под ним весь комплекс мероприятий, проводимых как на входе пользователя в систему, так и постоянно в течение его дальнейшей работы.

Здесь необходимо заострить внимание на методах аутентификации. Самый распространенный из них, конечно, парольный. Основные проблемы, которые сильно снижают надежность данного способа – это человеческий фактор. Даже если заставить пользователя использовать правильно сгенерированный пароль, в большинстве случаев его можно легко найти на бумажке в столе или под клавиатурой.

### 2.3 Защита документа

Базовый элемент любой СЭД — документ, внутри системы это может быть файл, а может быть запись в базе данных. Говоря о защищенном документообороте, часто подразумевают именно защиту документов, защиту той информации, которую они в себе несут. В этом случае все сводится к уже банальной (хотя и не простой) задаче защиты данных от несанкционированного доступа.

Здесь есть большое заблуждение, ведь речь идет именно о защите системы, а не только о защите данных внутри нее. Это значит, что нужно защитить также ее работоспособность, обеспечить быстрое восстановление после повреждений, сбоев и даже после уничтожения. Система — это как живой организм, не достаточно защитить только содержимое его клеток, необходимо защитить также связи между ними и их работоспособность. Поэтому к защите системы электронного документооборота необходим комплексный подход, который подразумевает защиту на всех уровнях СЭД. Начиная от защиты физических носителей информации, данных на них, и заканчивая организационными мерами.

Используя такой подход, можно построить систему, защищенную на всех уровнях, и рубежи обороны от угроз на каждом уровне. Возможно, выглядит немного параноидально, да и стоимость подобной защиты может сравняться со стоимостью самой СЭД, поэтому всегда нужно искать разумный баланс между безопасностью и стоимостью.

### 2.4 Обеспечение безопасного доступа

Этот момент обычно все понимают под безопасностью СЭД, чем часто ограничивают понятие безопасности систем. Безопасный доступ к данным внутри СЭД обеспечивается аутентификацией и разграничением прав пользователя.

Максимально надежный для проведения идентификации и последующей аутентификации способ — биометрический, при котором пользователь идентифицируется по своим биометрическим данным ( это может быть отпечаток пальца, сканирования сетчатки глаза, голос). Однако в этом случае стоимость решения выше, а современные биометрические технологии еще не настолько совершенны, чтобы избежать ложных срабатываний или отказов.

Еще один важный параметр аутентификации — количество учитываемых факторов. Процесс аутентификации может быть однофакторным, двухфакторным и т.д. Также возможно комбинирование различных методов: парольного, имущественного и биометрического. Так, например, аутентификация может проходить при помощи пароля и отпечатка пальца (двухфакторный способ).

### 2.5 Разграничения прав пользователя

В любой системе обязательно должно быть предусмотрено разграничение прав пользователя — и чем гибче и детальнее, тем лучше. Пусть потребуется большее время на настройку, но в итоге мы получим более защищенную систему. Разграничение прав внутри системы технически устраивают по-разному: это может быть полностью своя подсистема, созданная разработчиками СЭД, или подсистема безопасности СУБД, которую использует СЭД. Иногда их разработки комбинируют используя свои разработки и подсистемы СУБД. Такая комбинация предпочтительнее, она позволяет закрыть минусы подсистем безопасности СУБД, которые также имеют «дыры».

### 2.6 Конфиденциальность

Огромным преимуществом для конфиденциальности информации обладают криптографические методы защиты данных. Их применение позволят не нарушить конфиденциальность документа даже в случае его попадания в руки стороннего лица. Не стоит забывать, что любой криптографический алгоритм обладает таким свойством как криптостокойсть, т.е. и его защите есть предел. Нет шифров, которые нельзя было бы взломать — это вопрос только времени и средств. Кроме того, не стоит забывать об организационных мерах защиты. Какой бы эффективной криптография не была, ничто не помешает третьему лицу прочитать документ, например, стоя за плечом человека, который имеет к нему доступ. Или расшифровать информацию, воспользовавшись ключом который валяется в столе сотрудника. В настоящее время используется электронная цифровая подпись (ЭЦП) и шифрование. Эти средства реализуются при помощи асимметричной криптографии.

### 3 Шифрование с открытым ключом. АЛГОРИТМ RSA

### 3.1 Определение RSA

RSA (аббревиатура от фамилий Rivest, Shamir и Adleman) — криптографический алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших целых чисел. Криптосистема RSA стала первой системой, пригодной и для шифрования, и для цифровой подписи.

### 3.2 Криптосистема с открытым ключом

В криптосистеме с открытым ключом, в отличие от симметричной, используются два ключа: открытый и закрытый (закрытый хранится в секрете). Открытый ключ используется для проверки ЭЦП и для шифрования сообщений. Закрытый ключ – для генерации ЭЦП и для расшифрования сообщений.  
 ЭЦП – (Электронная цифровая подпись) – атрибут электронного документа, который получается в результате некоторого криптографического преобразования данных. ЭЦП позволяет проверить целостность документов, конфиденциальность документов, а так же идентифицировать владельца документа. Аналог обычной подписи.



Рисунок 1. Криптосистема с открытым ключом

### 3.3 Описание алгоритма RSA

В основе RSA лежит задача факторизации произведения двух простых больших чисел. Для шифрования используется простая операция возведения в степень по модулю N. Для расшифрования же необходимо вычислить функцию Эйлера от числа N, для этого необходимо знать разложение числа n на простые множители (В этом и состоит задача факторизации).

В RSA открытый и закрытый ключ состоит из пары целых чисел. Закрытый ключ хранится в секрете, а открытый ключ сообщается другому участнику, либо где-то публикуется.

### 3.3.1 Генерация ключей RSA

1. Выбираются два простых числа  (такие что  неравно );  
 2. Вычисляется модуль ;  
 3. Вычисляется значение функции Эйлера от модуля ;  
 4. Выбирается число e, называемое открытой экспонентой, число e должно лежать в интервале , а так же быть взаимно простым со значением функции ;

5. Вычисляется число d, называемое секретной экспонентой, такое, что  , то есть является мультипликативно обратное к числу  по модулю .

Итак, мы получили пару ключей:

Пара  - открытый ключ. Пара  - закрытый ключ.

### 3.3.2 Шифрование и расшифровывание в RSA

Пусть есть следующий сценарий:

Боб и Алиса переписываются в интернете, но хотят использовать шифрование, чтобы поддерживать переписку в секрете . Алиса заранее сгенерировала закрытый и открытый ключ, а затем отправила открытый ключ Бобу. Боб хочет послать зашифрованное сообщение Алисе:

Шифрование: Боб шифрует сообщение m, используя открытый ключ Алисы:

(1)

и отправляет сообщение Алисе.

Расшифровывание: Алиса принимает зашифрованное сообщение. Используя закрытый ключ , Алиса начинает расшифровывать сообщение

(2)

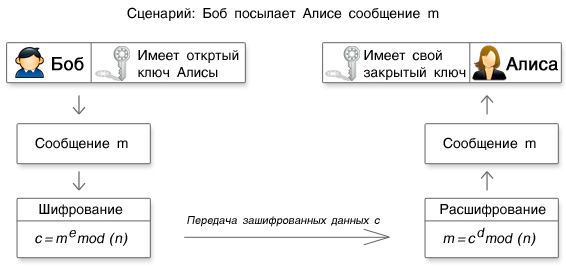


Рисунок 2. Боб посылает Алисе сообщение m

### 3.4 Безопасность схемы RSA

От каких параметров зависит стойкость алгоритма RSA? Представим себе, что к Бобу и Алисе присоединяется Ева, которая хочет узнать, какое сообщение послал Боб. Допустим, что у Евы есть открытый ключ Алисы  *(e,N)*, для того, чтобы расшифровать сообщение , необходимо знать закрытый ключ  *(d,N)*. Мы знаем, что

*,* (3)

однако Ева не знает, что:

 , (4)

т.е задача сводится к нахождению простых чисел  и  (хотя это не всегда так), которые связаны с известным  следующим образом .

Таким образом, чтобы алгоритм был стойким, необходимо:

1. Выбрать два больших простых случайных числа p и q (к примеру, >= 1024 бита каждое), должны быть не слишком различными и быть не слишком близкими;  
 2. Наибольший общий делитель  и  должен быть небольшим, лучший вариант, если делитель будет равняться двум;  
 3. Выбрать большое значение открытой экспоненты e, как правило, выбирают простые числа Ферма: 17, 257, 65537...;  
 4. Сохранение в секрете закрытого ключа.

### 3.5 Пример шифрования RSA

1. Выбираем простые числа (небольшие, чтобы упростить вычисления) ;  
 2. Вычисляем модуль ;  
 3. Вычисляем функцию Эйлера от ;  
 4. Выбираем открытую экспоненту ;  
 5. Определяем закрытую экспоненту .

Будем шифровать сообщение RSA, пусть букве соответствует цифра и т. д, тогда:

Открытый ключ:

;;;

.

**

Рисунок 3. Пример шифрования RSA

Используем закрытый ключ:

;;;

;

Получаем исходное сообщение - RSA.

### 3.6 Условие работы алгоритма

Необходимо проверить, удовлетворяет ли данный алгоритм требованиям к ассиметричным криптосистемам.

Условие:   
 Ассиметричный алгоритм шифрования является стойким, если атакующий имеет два открытых текста  и , а так же зашифрованный текст , не может с вероятностью большей, чем  определить к какому из сообщений  или  относится .

Проверка:  
 Перейдем к RSA и проверим условие. Вспомним ситуацию с Алисой и Бобом, допустим, канал связи прослушивает Ева. Боб спрашивает у Алисы: «Алиса, мы идем сегодня в кино», причем сообщение не шифруется. Алиса отвечает Бобу, но не хочет, чтобы кто-то знал, поэтому шифрует свой ответ на открытом ключе Боба и отправляет шифротекст Бобу. Ева перехватывает зашифрованное сообщение и знает, что Алиса ответила либо «Да», либо «Нет». Ева располагает открытым ключом Боба, поэтому последовательно шифрует сообщение «Да» и «Нет», соответственно одно из них совпадет с зашифрованным сообщением Алисы и Ева узнает, пойдет ли Алиса сегодня в кино или нет.

Из этого видно, что упрощенное описание алгоритма RSA не годится для практического использования. Решается эта проблема достаточно просто: к сообщению добавляется некоторая случайная величина, а затем полученный текст шифруется. Таким образом, если Ева перехватывает сообщение , то зашифровав «Да» и «Нет»:, будет видно, что  и  не совпадут.

Итак, в алгоритме RSA перед тем как зашифровать сообщение, к тексту добавляется некоторая случайная величина, а затем текст проходит процедуру шифрования. Поэтому функция шифрования принимает вид:

(5)

.

### ЗАКЛЮЧЕНИЕ

Таким образом Электронный документооборот позволяет реализовать безбумажный процесс передачи данных с помощью автоматизированных процессов обработки электронных документов. Наиболее широко он распространен на предприятиях, которые в последнее время просто не могут существовать без него.

Основной же проблемой с которой сталкиваются предприятия использующие ЭД, это реализация методов по обеспечению его безопасности. В настоящее время для защиты документов, в основном, используется электронная цифровая подпись (ЭЦП) и шифрование.

Алгоритмы ассиметричного шифрования используют как вспомогательный инструмент для передачи небольших объемов информации, к примеру секретных ключей симметричного шифра.

Такие гибридные системы получили широкое распространение и классический алгоритм RSA сейчас является частью множества других безопасных протоколов передачи данных.

### СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. В.М. Фомичев - Методы дискретной математики в криптологии, М.: Диалог-МИФИ, 2003.
2. Б. Шнайер - Прикладная криптография. Протоколы, алгоритмы и исходный код на C, 2-е издание, 2016.
3. А.П. Алферов, А.Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин - Основы криптографии, 2-е издание М.: Гелиос АРВ 2002.
4. [Л.М. Евдокимова](https://www.ozon.ru/person/21545578/), В.В. Корябкин,  [А.Н. Пыльки](https://www.ozon.ru/person/1541862/)н, О.Г. Швечкова -Электронный документооборот и обеспечение безопасности стандартными средствами windows: Учебное пособие, 2017.
5. И.К. Корнеев - Информационные технологии в работе с документами, 2016.