Учреждение образования

«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

**ЗАЩИТА ИНФОРМАЦИИ**

**И НАДЕЖНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ»**

**И «КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ**

**ЗАЩИТЫ ИНФОРМАЦИИ**

Студент: Бичун Н.Д.

ФИТ 3 курс 2 группа

Преподаватель: Ржеутская Н.В.

Минск 2022

# Практическое занятие №1

# Тема «РАЗРАБОТКА И ВНЕДРЕНИЕ

# ПОЛИТИКИ БЕЗОПАСНОСТИ

# ОРГАНИЗАЦИИ ИЛИ УЧРЕЖДЕНИЯ»

**Цель:** приобретение практических навыков разработки и внедрения эффективной политики информационной безопасности организации или учреждения.

**Задачи:**

1. Научиться выделять и классифицировать особенности информационной или информационно-вычислительной системы (ИВС)

конкретной организации или учреждения как объекта защиты.

2. Овладеть навыками принятия обоснованных решений по организационному и правовому регулированию проблем, относящихся к состоянию безопасности ИВС, обеспечению необходимого

уровня защиты информации в ИВС.

3. Овладеть основными приемами анализа угроз информационной безопасности ИВС.

4. Научиться выявлять все возможные угрозы и их источники

информационной безопасности в организации или учреждении,

анализировать и оценивать собранные данные.

5. Разработать концепцию, основные элементы политики безопасности для организации или учреждения по указанному преподавателем варианту задания.

6. Разработать мероприятия по внедрению предложенной Вами политики безопасности.

7. Результаты выполнения лабораторной работы оформить в

виде описания разработанной политики безопасности, а также

плана мероприятий по ее реализации.

Введение

Жизнь современного общества немыслима без современных информационных технологий. Компьютеры обслуживают банковские системы, контролируют работу атомных реакторов, распределяют энергию, следят за расписанием поездов, управляют самолетами, космическими кораблями. Компьютерные сети и телекоммуникации предопределяют надежность и мощность систем обороны и безопасности страны. Компьютеры обеспечивают хранение информации, ее обработку и предоставление потребителям, реализуя таким образом информационные технологии.

Однако именно высокая степень автоматизации порождает риск снижения безопасности (личной, информационной, государственной, и т.п.). Доступность и широкое распространение информационных технологий, ЭВМ делает их чрезвычайно уязвимыми по отношению к деструктивным воздействиям.

Информационная сфера имеет две составляющие: информационно-техническую (искусственно созданный человеком мир техники, технологий и т. п.) и информационно-психологическую (естественный мир живой природы, включающий и самого человека). Соответственно, в общем случае информационную безопасность общества (государства) можно представить двумя составными частями: информационно-технической безопасностью и информационно-психологической (психофизической) безопасностью.

Сущность информационно-технической безопасности можно определить, как достижение такого состояния развития общественных отношений, при котором обеспечена надежная и всесторонняя защита интересов субъектов этих отношений - человека, общ ества и государства - от угроз деструктивного информационного воздействия.

Информационно-психологическая безопасность состоит в том, что основным ее содержанием является защита интересов безопасности человека, безопасности общества и безопасности государства, как осознанная социальная потребность субъекта на безопасное удовлетворение своих потребностей.

3.1 Общие положения

***1. Цели и задачи***

Концептуальная схема информационной безопасности учебного учреждения направлена на защиту его информационных активов от угроз, исходящих от противоправных действий злоумышленников, уменьшение рисков и снижение потенциального вреда от аварий, непреднамеренных ошибочных действий персонала, технических сбоев, неправильных технологических и организационных решений в процессах обработки, передачи и хранения информации и обеспечение нормального функционирования технологических процессов.

Направление информационной безопасности создано в отделе собственной безопасности со следующими задачами и функциями, определяемыми постановлением Правительства 915-12 "О лицензировании отдельных видов деятельности" и Федеральным законом от 27 июля 2006 г. № 152-ФЗ «О персональных данных»:

**Основными разделами концепции информационной безопасности могут быть следующие:**

• определение ИБ (или СУИБ);

• структура информационной системы организации (учреждения) и вытекающая из этого структура системы обеспечения информационной безопасности;

• безопасность информации: принципы и стандарты;

• оценка рисков информационным ресурсам в организации

(учреждении);

• описание основных механизмов контроля безопасности;

• обязанности и ответственность каждого отдела, управления

или департамента, каждого сотрудника в реализации разработанной и утвержденной политики безопасности;

• обязанности лица (администратора безопасности), ответственного за организацию оперативного контроля и управления политикой безопасности;

***2. Организационно-правовой статус сотрудников информационной безопасности***

- сотрудники имеют право беспрепятственного доступа во все помещения, где установлены технические средства с Информационными системами, право требовать от руководства подразделений и администраторов ИС прекращения автоматизированной обработки информации, персональных данных, при наличии непосредственной угрозы защищаемой информации;

- имеют право получать от пользователей и администраторов необходимую информацию по вопросам применения информационных технологий, в части касающейся вопросов информационной безопасности;

- главный специалист по ИБ имеет право проводить аудит действующих и вновь внедряемых ИС, ПО, на предмет реализации требований защиты и обработки информации, соответствию требований законодательства, запрещать их эксплуатацию, если не отвечают требованиям или продолжение эксплуатации может привести к серьезным последствиям в случае реализации значимых угроз безопасности;

-сотрудники имеют право контролировать исполнение утвержденных нормативных и организационно-распорядительных документов, касающихся вопросов информационной безопасности.

3.2 Структура организации

Общая структура организации школы

Первый уровень структуры – уровень директора (по содержанию – это уровень стратегического управления). Директор школы определяет совместно с Советом школы, Управляющим советом стратегию развития школы, представляет еѐ интересы в государственных и общественных инстанциях. Общее собрание трудового коллектива согласовывает Программу развития школы. Директор школы несет персональную юридическую ответственность за организацию жизнедеятельности школы, создает благоприятные условия для развития школы.

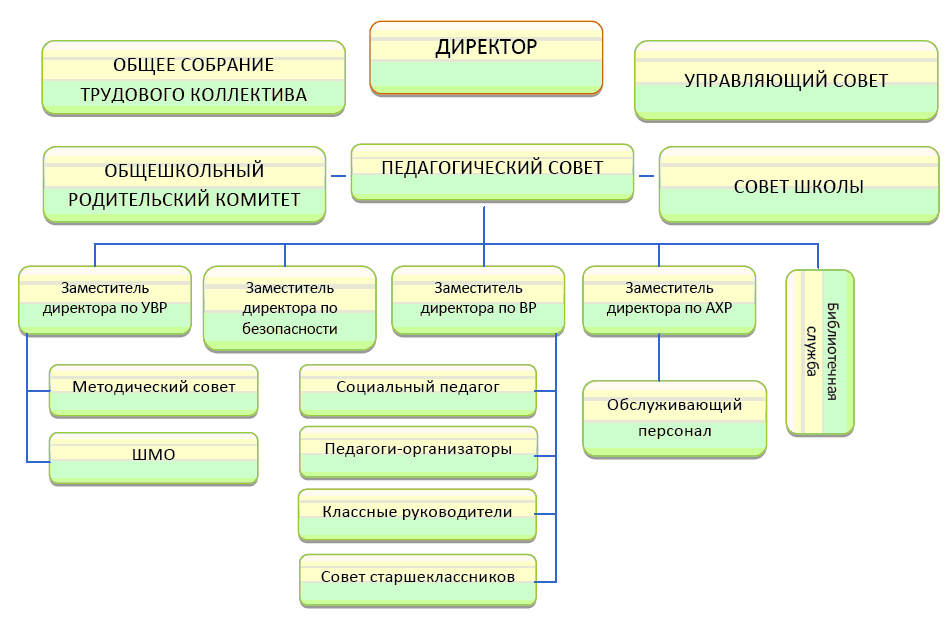
На втором уровне структуры (по содержанию – это тоже уровень стратегического управления) функционируют традиционные субъекты управления: Совет школы, Управляющий совет, педагогический совет, родительский комитет, общее собрание трудового коллектива, профсоюзный комитет.

Третий уровень структуры управления (по содержанию – это уровень тактического управления) – уровень заместителей директора. Этот уровень представлен также методическим советом. Методический совет – коллегиальный совещательный орган, в состав которого входят руководители школьных методических объединений. Педагогический коллектив работает по единой научно-методической теме: «Обновление содержания образования и форм организации учебно-воспитательного процесса в условиях перехода основного и среднего образования на ФГОС. 2015 - 2018 гг.».

Четвертый уровень организационной структуры управления – уровень учителей, функциональных служб (по содержанию – это уровень оперативного управления), структурных подразделений школы. Методические объединения – структурные подразделения методической службы школы, объединяют учителей одной образовательной области.

Пятый уровень организационной структуры – уровень обучающихся. По содержанию – это тоже уровень оперативного управления, но из-за особой специфичности субъектов этот уровень скорее можно назвать уровнем «самоуправления». Иерархические связи по отношению к субъектам пятого уровня предполагают курирование, помощь, педагогическое руководство.

В школе созданы органы ученического самоуправления, детские общественные организации. Органы ученического самоуправления действуют на основании утвержденных Положений.



3.3 Оценка рисков

Угрозы информационной безопасности могут быть классифицированы по различным признакам:

– по аспекту информационной безопасности, на который направлены угрозы:

а) угрозы конфиденциальности (неправомерный доступ к информации);

б) угрозы целостности (неправомерное изменение данных);

в) угрозыдоступности (осуществление действий, делающих невозможным или затрудняющих доступ к ресурсам информационной системы);

– по степени преднамеренности действий:

а) случайные (неумышленные действия, например, сбои в работе систем, стихийные бедствия);

б) преднамеренные (умышленные действия, например, шпионаж и диверсии);

– по расположению источника угроз:

а) внутренние (источники угроз располагаются внутри системы);

б) внешние (источники угроз находятся вне системы);

– по размерам наносимого ущерба:

а) общие (нанесение ущерба объекту безопасности в целом, причинение значительного ущерба);

б) локальные (причинение вреда отдельным частям объекта безопасности);

в) частные (причинение вреда отдельным свойствам элементов объекта безопасности);

– по степени воздействия на информационную систему:

а) пассивные (структура и содержание системы не изменяются);

б) активные (структура и содержание системы подвергается изменениям).

Основными угрозами являются:

– несанкционированное вмешательство в управление технологическими процессами;

– нарушение функционирования структуры или ее отдельных элементов;

– несанкционированный доступ к информации, хранимой в базах данных АСУ ТП и передаваемой по каналам передачи данных.

В результате реализации угроз ИБ могут быть нарушены:

– целостность (утрата, уничтожение, модификация) информации;

– доступность (блокирование) информации и отдельных элементов АСУ ТП;

– конфиденциальность (утечка, перехват, съем, копирование, хищение, разглашение) информации.

Обеспечение ИБ осуществляется по следующим направлениям, реализуемым организационно-техническими мерами защиты.

Физическая защита, включая:

– защиту технических средств обработки, хранения и передачи информации;

– защиту зданий, сооружений и помещений.

Обеспечение ИБ при эксплуатации средств обработки, хранения и передачи информации и использовании информационных ресурсов, включая:

– защиту от вредоносного ПО;

– резервирование серверов, сетевого оборудования, средств защиты и каналов передачи данных;

– обеспечение безопасности сетевой инфраструктуры;

– защиту программного обеспечения;

– регистрацию и учет событий ИБ;

– организацию безопасного использования, преобразования, хранения и передачи информации;

– криптографическую защиту.

Контроль доступа, в том числе:

– управление доступом пользователей;

– определение ответственности пользователей;

– контроль доступа к прикладным системам;

– контроль доступа к ОС;

– контроль сетевого доступа;

– обеспечение безопасности при использовании мобильных устройств;

– обеспечение безопасности в беспроводных сетях;

– контроль доступа к сетевому оборудованию.

Реализация организационно-технических мер обеспечения ИБ достигается в первую очередь путем:

– наделения пользователей автоматизированной системы управления технологическими процессами правами доступа и привилегиями по работе в АСУ ТП;

– корректного использования и администрирования встроенных механизмов безопасности технических средств обработки, хранения и передачи информации и средств защиты;

– контроля функционирования и настроек механизмов безопасности, а также соблюдения требований по ИБ;

– физической защиты технических средств обработки, хранения и передачи информации от неправомерного доступа к ним.

Обязанности пользователей по обеспечению ИБ зависят от занимаемой должности и определены в их должностных инструкциях.

**3.3 Защита технических средств обработки, хранения и передачи информации**

В целях предотвращения несанкционированного доступа к информации и ее утечки, хищения технических средств обработки и хранения информации и несанкционированного управления ими, а также простоев в функционировании АСУ ТП обеспечивается физическая защита входящих в нее технических средств. Серверное оборудование и критичное сетевое оборудование размещаются в запираемых шкафах с сигнализацией, располагаемых в специализированных помещениях (серверных), ограничивающих доступ к ним посторонних лиц. Перед утилизацией или передачей в ремонт технических средств выполняется гарантированное удаление информации с них. Кабельные сети прокладываются так, чтобы максимально ограничить несанкционированный доступ к ним. Для защиты от перебоев электричества в эксплуатацию вводятся централизованные системы бесперебойного питания. Система ИБ включает в себя максимальное количество элементов, обеспечивающих эффективную защиту системы при критической нагрузке.

3.4. Организация безопасной эксплуатации средств обработки, хранения и передачи информации

Функции по администрированию и контролю эксплуатации средств обработки, хранения и передачи информации разделяются и возлагаются на специально выделенных для этого работников. Изменения конфигурации средств обработки и хранения информации, а также изменения сетевой инфраструктуры, конфигурации сетевого оборудования выполняются администратором. Все изменения регистрируются в соответствующих журналах. Самостоятельное изменение конфигурации средств обработки, хранения и передачи информации пользователями АСУ ТП запрещено. Использование съемных носителей информации в автоматизированной системе управления технологическими процессами запрещено. При размещении средств разработки, тестирования и эксплуатации обеспечивается их физическое или логическое разделение в целях снижения риска несанкционированного доступа или внесения изменений в систему.

3.4.1 Защита от вредоносного программного обеспечения

В целях предотвращения проникновения, обнаружения внедрения и нейтрализации вредоносного ПО в АСУ ТП применяются средства защиты от вредоносного ПО. Средства защиты от вредоносного ПО устанавливаются на серверном оборудовании и АРМ операторов и специалистов автоматизированной системы управления технологическими процессами. Управление и обновление средств защиты от вредоносного ПО осуществляются централизованно. Разрешается использование только сертифицированных на соответствие требованиям безопасности информации средств защиты от вредоносного ПО. Администрирование средств защиты от вредоносного ПО осуществляется системным администратором. Настройки системы защиты от вредоносного ПО согласовываются и контролируются администратором ИБ.

Используемая антивирусная система защиты имеет:

– стойкую систему самозащиты, которая не позволит неизвестной вредоносной программе нарушить нормальную работу АСУ ТП и сделает возможным функционирование АСЗ до поступления обновления;

– систему обновлений, находящуюся под контролем системы самозащиты антивирусной системы и не использующую компоненты операционной системы, которые могут быть скомпрометированы;

– систему обновления, позволяющую мгновенно, по сигналу системы централизованного управления доставить на защищаемый антивирусом объект обновления для лечения активного заражения;

– дополнительные механизмами для обнаружения новых неизвестных вредоносных программ;

– проверяет все поступающие из локальной сети файлы до момента получения их используемыми приложениями, что исключает использование вредоносными приложениями неизвестных уязвимостей данных приложений;

– систему централизованного сбора информации с удаленных рабочих станций и серверов, позволяющую максимально быстро передавать в антивирусную лабораторию всю необходимую для решения проблемы информацию.

3.4.2 Обеспечение безопасности сетевой инфраструктуры

В целях обеспечения непрерывного и устойчивого функционирования АСУ ТП осуществляется защита ее сетевой инфраструктуры. Защита сетевой инфраструктуры обеспечивается:

– физической защитой сетевого оборудования и средств защиты;

– контролем логического доступа к сетевому оборудованию;

– шифрованием каналов управления;

– контролем сетевых соединений;

– обнаружением и предотвращением вторжений;

– мониторингом подключаемых к ЛВС автоматизированной системы управления технологическими процессами сетевых устройств;

– использованием встроенных в сетевое оборудование средств защиты от подмены адреса (средств антиспуфинга);

– защитой информации ограниченного доступа при ее передаче вне контролируемых зон;

– применением средств мониторинга и регистрации событий.

Контроль сетевых соединений между ЛВС АСУ ТП и подключаемыми к ней беспроводными сетями также осуществляется средствами межсетевого экранирования. Защита информации ограниченного доступа при ее передаче вне контролируемых зон осуществляется применением сертифицированных средств криптографической защиты информации (построением защищенных виртуальных сетей). Защита от вторжений в ЛВС АСУ ТП осуществляется средствами обнаружения и предотвращения вторжений, размещаемыми на входе в ЛВС. Базы данных сигнатур средств обнаружения и предотвращения вторжений регулярно обновляются с сайта производителя применяемых средств. Категорически запрещается удаленное администрирование АСУ ТП.

В целях поддержания работоспособности ПО осуществляются меры по устранению уязвимостей ПО, а также другие меры защиты от:

– умышленного либо неумышленного раскрытия, модификации или уничтожения защищаемых данных. В частности, это подразумевает использования средств ограничения доступа к различным ресурсам офисного контроля;

– установки средств защиты кем-либо, кроме администратора, несанкционированного внесения изменений в порядок функционирования системы защиты, изменения ее возможностей. Данное требование приводит к необходимости разграничения прав доступа к настройкам системы, защите ее от несанкционированного воздействия. Это подразумевает использование в локальной сети только программных продуктов, поддерживающих ролевой принцип доступа, а также применение функций офисного контроля. Средства защиты должны устанавливаться как на рабочие станции, так и на сервер. В организации, соответствующей требованиям стандарта, должна использоваться только защищенная почта, что вместе с требованием о наличии защиты от вирусов и спама подразумевает установку средств антивирусной фильтрации почтовых сообщений. В свою очередь доступ в сеть Интернет должен использоваться только для обеспечения банковской деятельности. Устранение уязвимостей ПО достигается регулярным централизованным получением и установкой обновлений, предоставляемых разработчиками ПО. Обновление ОС, другого общесистемного и прикладного ПО осуществляется системными администраторами и администраторами прикладных систем. Обновления для ПО АСУ ТП получаются с серверов обновлений, размещенных в ИУС ПХД.

3.4.3 Криптографическая защита

В целях обеспечения конфиденциальности информации при ее передаче вне контролируемых зон применяются сертифицированные установленным порядком средства криптографической защиты информации. Это специальные методы шифрования, кодирования в результате которых содержание передаваемых файлов становится недоступным, без предъявления ключа криптограммы и обратного преобразования. Криптографическая защита информации на предприятии реализована с помощью метода криптосистемы с открытым ключом. В системе с открытым ключом используются два ключа — открытый и закрытый, которые математически связаны друг с другом. Информация шифруется с помощью открытого ключа, который доступен всем желающим, а расшифровывается с помощью закрытого ключа, известного только получателю сообщения.

Для построения политики ИБ рассматривают следующие направления защиты ИВС:

• защита объектов ИВС;

• защита процессов, процедур и программ обработки информации;

• защита каналов связи;

• подавление побочных электромагнитных излучений;

• управление системой защиты.

Организационная защита обеспечивает:

• организацию охраны, режима, работу с кадрами и с документами;

• использование технических средств безопасности (например,

простейших дверных замков, магнитных или иных карт и др.), информационно-аналитическую деятельность по выявлению внутренних и внешних угроз.

**Общие положения ИБ**

К числу физических мер относятся:  
  
реализация пропускной системы для доступа в помещения, в которых находятся носители данных;  
создание системы контроля и управления доступом;  
определение уровней допуска;  
создание правил обязательного регулярного копирования критически важных данных на жесткие диски ПК, не подключенных к интернету.  
Также среди физических мер можно назвать правила по созданию паролей и их периодической замене  
разрешенные антивирусы и другие виды специального софта.  
  
Применяемое для технической защиты программное обеспечение должно обеспечивать контроль электронной почты, которой пользуются ученики или персонал образовательной организации. Также могут устанавливаться ограничения на копирование данных с жестких дисков компьютеров. Обязательно рекомендуется использование контент-фильтра, с помощью которого ограничивается доступ детей к определенным ресурсам в интернете.

* Культура безопасности  
  Одной из задач педагогического коллектива ОУ является формирование у учащихся особых поведенческих мотивов, связанных с предотвращением угроз для их жизни и Для этого учителям необходимо формировать у своих воспитанников культуру безопасности.

3.5 Сетевая безопасность

***3.5.1 Доступ из Интернет в сеть Учебного учреждения:***

- доступ во внутреннюю сеть осуществляется только через настроенный межсетевой экран;

- доступ из вне периметра сети разрешен только по распоряжению директора ЦНИТ с согласованием у ответственного сотрудника ОСБ, по определенному порту и на определенное время;

- не допускается удаленный доступ в локальную сеть с использованием не персонифицированных, групповых и анонимных учетных записей;

- не допускается использование программ удаленного администрирования типа TeamViewer. Как исключение, по согласованию с сотрудником ИБ ОСБ возможно подключение для удаленной настройки ПО на ограниченное время. Настройка и конфигурация средств обнаружения вторжений, межсетевых экранов должны обеспечивать оперативное обнаружение несанкционированного доступа к ресурсам сети для принятия мер блокирования проникновения нейтрализации последствий.

При администрировании удаленного доступа к ресурсам корпоративной сети Учебного учреждения предъявляются следующие требования:

- удаленный доступ пользователей к ресурсам и сервисам компьютерной сети Учебного учреждения обеспечивается на основе зарегистрированных персональных учетных записей, с использованием технологии VPN, других протоколов шифрования;

- доступ предоставляется сроком на 3 месяца, при необходимости продлевается с разрешения директора ЦНИТ;

- делается соответствующая запись в Журнале учета предоставления удаленного доступа; - список сотрудников, которым предоставлен удаленный доступ поддерживается в актуальном состоянии и передается в ОСБ по запросу.

В целях обеспечения безопасности и нормального функционирования компьютерных сетей запрещается:

- самовольно подключать компьютерное оборудование (беспроводные точки доступа, маршрутизаторы, компьютеры и др.) к сети Учебного учреждения и присваивать ему сетевое имя и адрес без согласования с ЦНИТ;

- перемещать компьютеры между сетевыми розетками и другими коммуникационными устройствами без согласования с ЦНИТ;

- использовать информационные ресурсы Учебного учреждения для сетевых игр, распространения коммерческой рекламы; организации СПАМа. - сканировать узлы сети неуполномоченными на то сотрудниками . 2.2. Средства защиты, маршрутизаторы и межсетевые экраны:

Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. N 21 определяет как необходимость организацию управления (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы. В Университете используется система межсетевого экранирования, которая реализует функции фиксации во внутренних журналах информации о проходящем IP-трафике, фильтрацию пакетов служебных протоколов, блокирования доступа не идентифицированного объекта.

Для анализа защищенности ИС сотрудниками ИБ ОСБ применяются специализированные программно-аппаратные средства – сканеры безопасности. Проводится выявление и анализ уязвимостей и несоответствия в настройках ОС, ПО, СУБД, сетевого оборудования.

Выявленные уязвимости протоколируются и передаются в ЦНИТ для устранения в установленные сроки. Запрещается использовать ПО снятое с поддержки, имеющее уязвимости, с просроченными сертификатами. Подсистема обнаружения вторжений, обеспечивает выявление сетевых атак на элементы ИС подключенные к сетям общего пользования и (или) международного обмена. Функционал подсистемы реализуется программными и программноаппаратными средствами, на межсетевых экранах.

Администратор сети ведет протоколирование и регулярный мониторинг доступа, контролирует содержание трафика с использованием специализированного ПО, проводит анализ логфайлов. На межсетевом экране заводится лог-файл, куда записываются все обращения к ресурсам (попытки создания соединений). Доступ к лог-файлам имеют администратор сети и сотрудник ОСБ. Анализ лог-файлов проводится с применением соответствующего ПО (анализатор логов) сотрудником ОСБ Сотрудник ИБ ОСБ должен иметь независимый доступ к элементам системы защиты для контроля настроек конфигураций, просмотра системных журналов . Доступ из одного сегмента сети в другой ограничивается и разделяется маршрутизаторами. Настройкой маршрутизаторов занимается отдел сетевого и системного администрирования. Приобретение и установка средств и систем защиты ИС осуществляются по согласованию с сотрудником ИБ ОСБ. Сеть ИСПДн выделена в отдельный сегмент и защищена межсетевым экраном.

3.6 Локальная безопасность

***3.6.1 Антивирусная защита***

Исходя из требований ФСТЭК от 30 июля 2012 г. № 240/24/3095 к средствам антивирусной защиты антивирусное ПО должно соответствовать 6 классу защиты и типу «А» для применения в информационных системах персональных данных 4 класса.

Антивирусная защита предназначена для обеспечения антивирусной защиты серверов и АРМ пользователей Учебного учреждения. На каждом работающем компьютере, или сервере при вводе в эксплуатацию или после переустановки ОС сотрудниками ЦНИТ в обязательном порядке устанавливается и активируется антивирусная программа.

Установка средств антивирусного контроля (в том числе настройка параметров средств антивирусного контроля) на АРМ, серверах, осуществляется специалистами структурных подразделений и ЦНИТ в соответствии с руководствами по применению конкретных антивирусных средств. Отключение или не обновление антивирусных средств не допускается.

Установка и обновление антивирусных средств в организации контролируется централизованно ответственным сотрудником ЦНИТ. Система обнаружения атак, встроенная в антивирусную программу, сохраняет информацию об атаках и подозрительной активности в лог-файлы, которые анализирует ответственный сотрудник ЦНИТ и высылает генерируемые системой отчеты о сетевых атаках и вирусной активности сотруднику ИБ ОСБ.

В случае массированной вирусной атаки сотрудники ЦНИТ определяют масштаб заражения, принимают меры к локализации, блокированию распространения, совместно с сотрудником ИБ ОСБ определяют источник заражения, характер действия и распространения вируса, нейтрализуют последствия атаки. При необходимости ставятся патчи и необходимые обновления ПО, закрывающие уязвимости, используемые вирусами. Пользователи руководствуются требованиями антивирусной защиты, изложенными в Правилах использования информационных систем и ИТсервисов ТГУ.

***3.6.2 Защита электронного документооборота.***

Передача информации конфиденциального характера за периметр сети осуществляется только по защищенным каналам. Защищенные каналы строятся с 10 использованием криптозащиты, на базе решений VipNet, VPN, Банк-клиент или других, сертифицированных ФСТЭК. Криптографическая защита предназначена для исключения НСД к защищаемой информации, при ее передачи по каналам связи сетей общего пользования и (или) международного обмена. Криптографическая защита реализуется путем внедрения криптографических программно-аппаратных комплексов КриптоПро . Все экземпляры КриптоПро должны иметь лицензию и регистрируются в Журнале СКЗИ у сотрудника ИБ ОСБ. Электронные подписи выдаются удостоверяющим центром на определенное лицо, по его документам на основании заключенного договора. Инициатором заключения договора является структурное подразделение. После получения ключа ЭП, снимается копия сертификата и регистрируется в журнале учета СКЗИ у сотрудника ИБ ОСБ. Ключи электронных подписей должны храниться в сейфах ответственных лиц. Доступ неуполномоченных лиц к носителям ключей должен быть исключен.

Передача ключей запрещена. Запрещается оставлять носители с ЭП установленными в компьютер, при покидании рабочего места. Компьютеры, на которых установлены средства криптозащиты, должны соответствовать требованиям, изложенным в документации по КриптоПро. Соответствующий документации объем работы проводит сотрудник ЦНИТ по служебной записке сотрудника ИБ ОСБ. Внутренний документооборот является подсистемой ИСПДн, осуществляется в защищенном исполнении с использованием ПО, для которого актуальны угрозы 3-го типа, связанные с наличием НДВ в ПО.

Разграничение прав доступа к информационным системам и системам хранения данных, защита от НСД Для доступа к информационным системам Учебного учреждения сотрудник должен ввести логин и пароль. При предоставлении доступа к ОС, приложениям ИС, реализуется принцип минимума привилегий доступа. В целях защиты информации организационно и технически разделяются подразделения Учебного учреждения, имеющие доступ и работающие с различной информацией (в разрезе ее конфиденциальности и смысловой направленности). Данная задача решается с использованием возможностей конкретных ИС, где в целях обеспечения защиты данных доступ и права пользователей ограничивается набором прав и ролей. В случае обработки информации конфиденциального характера права назначаются администратором ИС по ролевой матрице доступа, в соответствии с функциональными обязанностями, определяемыми должностью и по служебной записке руководителя подразделения согласованной с сотрудником ОСБ. 11 Администратором ИС проводится анализ журналов доступа к ресурсам ИС, фиксируются попытки НСД, о которых докладывается ответственному сотруднику ИБ ОСБ. Для защиты от НСД на компьютерах в сегментах сети, где обрабатывается информация конфиденциального характера используются продукты линейки Dallas Lock, Secret Net, c администрированием в Центре безопасности, развернутом в домене. Администратором Центра безопасности является администратор домена. Не допускается использование учетных записей уволенных сотрудников.

***3.6.3 Использование электронной почты, сети Интернет***

Не допускается распространять материалы, использование и распространение которых ограничено действующим законодательством РФ.

Пересылка информации конфиденциального характера осуществляется только с использованием корпоративной почты.

Электронная почта на рабочем месте сотрудника используется только для служебной, и иной, предусмотренной должностными обязанностями переписки.

Логин и пароль к корпоративной электронной почте для сотрудников выдает ответственный сотрудник ЦНИТ по служебной записке на имя директора ЦНИТ, для студентов – по студенческому билету.

Запрещается открывать письма с подозрительными вложениями, с незнакомого адреса и.т.п., о получении подобных писем сообщается сотруднику ИБ ОСБ. Запрещается публиковать информацию конфиденциального характера в социальных сетях, пересылать через системы мгновенного обмена сообщениями (ICQ, Jabber и. т. п.).

Запрещается использование облачных сервисов на рабочих местах сотрудников, обрабатывающих информацию конфиденциального характера.

Доступ через беспроводную сеть разрешается только к общедоступным ресурсам сети.

Беспроводные точки устанавливают и администрируют сотрудники ЦНИТ. Самостоятельно скачивать и устанавливать программное обеспечение разрешается только уполномоченным на то сотрудникам ЦНИТ. Запрещается несогласованная с ЦНИТ установка роутеров WiFi.

3.7 Физическая защита

Все объекты критичные с точки зрения информационной безопасности (сервера баз данных, маршрутизаторы ) находятся в контролируемых зонах. Сотрудники ЦНИТ обязаны вскрывать и сдавать под охрану помещение серверной в соответствии с Инструкцией по вскрытию и сдаче под охрану помещения серверной. 12 Порядок доступа сотрудников ЦНИТ определяется Порядком доступа в серверные помещения. При неавтоматизированной обработке информации конфиденциального характера документы (личные дела сотрудников, студентов, абитуриентов, карточки лицевых счетов, картотека и.т.д.) должны храниться в шкафах, исключаемых несанкционированный доступ к ним. Требования к обеспечению безопасности определены в документе Порядок доступа в помещения, в которых обрабатывается информация конфиденциального характера. В контролируемых зонах Учебного учреждения ведется видеонаблюдение. На территории Учебного учреждения действует пропускной режим, порядок которого определяется локальным нормативным актом.

**3.8 Обработка персональных данных**

Необходимая нормативная и организационно-регламентирующая документация размещена на сайте Отдела собственной безопасности. Все сотрудники Учебного учреждения, являющиеся пользователями ИСПДн, должны четко знать и строго выполнять установленные внутренними нормативными документами правила и обязанности по доступу к защищаемым объектам и соблюдению принятого режима безопасности обработки ПДн. Компетентность пользователей в области обеспечения ИБ достигается обучением правилам безопасной (с точки зрения ИБ) работы, осведомленности об источниках потенциальных угроз и периодическими проверками их знаний и навыков.

Занятия с пользователями проводятся сотрудником ИБ ОСБ на регулярной основе не реже двух раз в год. Все действия пользователей компьютеров и обязанности по соблюдению требований ИБ определяются Порядком действий пользователя информационной системы по обеспечению информационной безопасности в Тольяттинском государственном университете, который они изучают, имеют распечатанный экземпляр с подписью сотрудника об ознакомлении.

При допуске сотрудника к выполнению обязанностей связанных с обработкой персональных данных непосредственный начальник подразделения, в которое он поступает, организует ознакомление с должностной инструкцией и необходимыми документами, регламентирующими требования по защите ПДн, подает служебную записку директору ЦНИТ о предоставлении доступа к ИСПДн с указанием предполагаемой роли сотрудника. Далее сотрудник проходит инструктаж у администратора безопасности ИСПДн, и расписывается об ознакомлении с Положением о защите персональных данных и Порядком обеспечения конфиденциальности при обработке персональных данных, получает у администратора ИСПДн логин и пароль к учетной записи с правами, согласно ролевой матрицы доступа. Порядок работы с запросами на предоставление сведений по персональным данным определяется утвержденными локальными нормативными документами. 13

Общедоступными персональными данными сотрудников являются фамилия, имя, отчество, занимаемая должность, подразделение, а студентов, аспирантов, слушателей - фамилия, имя, отчество, группа, специальность. Сотрудники Учебного учреждения должны обеспечивать надлежащую защиту оборудования, оставляемого без присмотра, особенно в тех случаях, когда в помещение имеют доступ посторонние лица.

Сотрудникам, обрабатывающим ПДн, запрещается устанавливать любое программное обеспечение, подключать личные мобильные устройства и отчуждаемые незарегистрированные в ОСБ носители информации, а так же записывать на них защищаемую информацию, за исключением случаев, предусмотренных функциональными обязанностями.

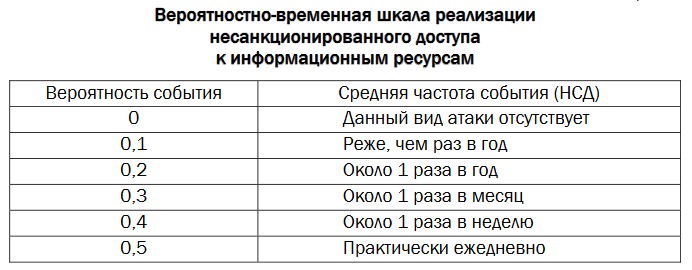
Сотрудникам запрещается разглашать содержание защищаемой информации, которая стала им известна при работе с информационными системами Учебного учреждения, третьим лицам, согласно Положения о защите персональных данных. Запрещается хранение информации конфиденциального характера локально на компьютере, не оснащенном программными средствами предотвращения несанкционированного доступа (SecretNet, DallasLock и др.) Допуск к ИСПДн третьих лиц для осуществления ими договорных обязательств осуществляется при выполнении требований, предъявляемых к защите информации и соблюдения конфиденциальности, отражаемых в договоре, согласованном с ОСБ на этапе заключения. СКЗИ при обработке персональных данных в университете не используются. Текст Политики в отношении обработки персональных данных размещается на сайте ОСБ в свободном доступе.

**Оценка угроз, рисков и уязвимостей.**

Анализ ценности ресурсов, оценка значимости угроз, а также эффективности существующих и планируемых средств защиты (воспользуйтесь приведенными в описании таблицами, заполните их).

**Условная численная шкала для оценки ущерба учреждения**

|  |  |
| --- | --- |
| Величина ущерба | Описание |
| 0 | Раскрытие информации, не являющейся конфиденциальной и не раскрывающая данных о работниках и учениках |
| 1 | Ущерб атаки есть, но он незначителен и не связан с положением учреждению |
| 2 | Существует вероятность потери некоторого числа работников или учеников, учреждение теряет часть прибыли |
| 3 | Потеря весомой доли работников или учеников и потеря доверия, учреждение несет убытки |
| 4 | Полная потеря доверия и конкурентоспособности, долги, а так же полная потеря доли работников и учеников , банкротство |
| 5 | Полное банкротство учреждения и прекращение существования |

****

**Оценка рисков**

|  |  |  |  |
| --- | --- | --- | --- |
| Описание атаки | Ущерб | Вероятность | Риск |
| Откл. света | 1 | 0,3 | 0,3 |
| Поломка техники учениками | 2 | 0,2 | 0,4 |
| Атаки на сервер | 3 | 0,1 | 0,3 |
| Перехват данных | 3 | 0,1 | 0,3 |
| Кража информации | 3 | 0,2 | 0,6 |
| Потеря информации с печатных носителей | 3 | 0,2 | 0,6 |
| Восстановление | 3 | 0,1 | 0,3 |
| Обвал базы данных | 1 | 0,1 | 0,1 |
| Итого |  | | 2,9 |

Заключение

Политика безопасности — совокупность документированных управленческих решений, направленных на защиту информации и ассоциированных с ней ресурсов. Основная цель политики безопасности – определение технических требований к защите компьютерных систем и сетевой аппаратуры, способы настройки систем администратором с точки зрения их безопасности.

На политике безопасности нельзя экономить, так как данные, которые могут быть подвержены хищению, копированию или изменению, могут стоить дороже, чем ресурсы, потраченные на её разработку и осуществление.

Разработаны технические меры обеспечения безопасности, организационные меры обеспечения безопасности, сетевая безопасность, общие меры предосторожностей, так же такие пункты как люди, и процессы, и избыточность, и непрерывность работы.

Политика безопасности должна быть разработана так, чтобы её взлом стоил дороже, чем сама информация.

**Вывод:** в ходе лабораторной работы был разработан проект политики информационной безопасности учебного учреждения.

Практическое занятие №2

Тема «ЭЛЕМЕНТЫ ТЕОРИИ ИНФОРМАЦИИ. ПАРАМЕТРЫ И ХАРАКТЕРИСТИКИ ДИСКРЕТНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

**Цель:** приобретение практических навыков расчета и анализа

параметров и информативных характеристик дискретных ИС.

**Задачи:**

1. Закрепить теоретические знания по основам теории информации.

2. Разработать приложение для расчета и анализа параметров

и информативных характеристик дискретных ИС.

3. Результаты выполнения лабораторной работы оформить в

виде описания разработанного приложения, методики выполнения

экспериментов с использованием приложения и результатов эксперимента.

**Общие понятия**

**Основные характеристики и параметры двоичных систем.**

Важнейшая характеристика источника, получателя или канала – **алфавит**.

Алфавит, А – это общее число знаков или символов (N), используемых для генерации или передачи сообщений. Символы алфавита будем обозначать через {аi}, где 1 ≤ i ≤ N; N – мощность алфавита. Минимальное число элементов алфавита Nmin = 2, А = {0, 1} – двоичный код.

Информационной характеристикой алфавита (источника сообщений на основе этого алфавита) является **энтропия**.

Энтропию алфавита ***А*** = {*ai*} по К. Шеннону рассчитывают по следующей формуле:

*N*

*HS* ( *A*)   *P*(*ai* )  log2 *P*(*ai* ).

*i*1

энтропия алфавита показывает, какое количество информации приходится в среднем на один символ алфавита.

= Энтропия Хартли. Если для каждого символа одинаковый алфавит

*HCh* ( *A*) = log2 *N*.

Сообщение *Хk*, которое состоит из *k* символов, должно харак- теризоваться определенным *количеством информации I*(*Хk*):

*I* ( *Xk* )  *H* ( *A*)  *k*.

Если вероятность ошибки в ДСК отлична от 0 (*р* > 0), пере- данное сообщение может содержать ошибки: *Хk* ≠ *Yk.* Количество информации в таком сообщении при его передаче по ДСК будет определяться не энтропией двоичного алфавита (в соответствии с выражением (2.3)), а эффективной энтропией *Hе*(*A*) алфавита или пропускной способностью канала:

*He* ( *A*)  1  *H* (*Y* | *X* ),

где *H*(*Y* | *X*) *–* условная энтропия:

*H* (*Y* | *X* )  *p*  log2 *p*  *q*  log2 *q*.

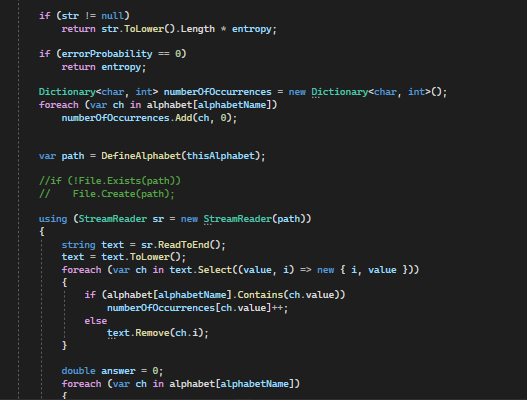
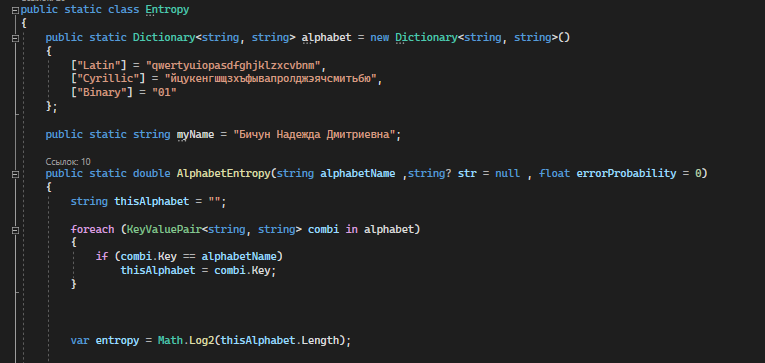
**Практическое задание**

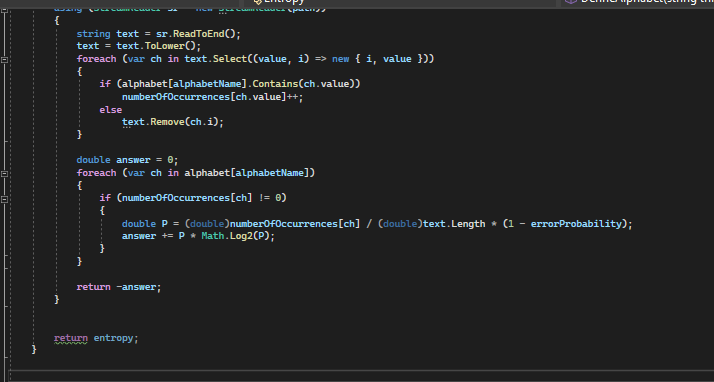
а) рассчитать энтропию указанных преподавателем алфавитов: один – на латинице, другой – на кириллице (по формуле (2.1) перейти от частоты появления каждого символа алфавита к соответствующей вероятности); в качестве входного может быть принят произвольный электронный текстовый документ на основе соответствующего алфавита; частоты появления символов алфавитов оформить в виде гистограмм (можно воспользоваться приложением MS Excel);

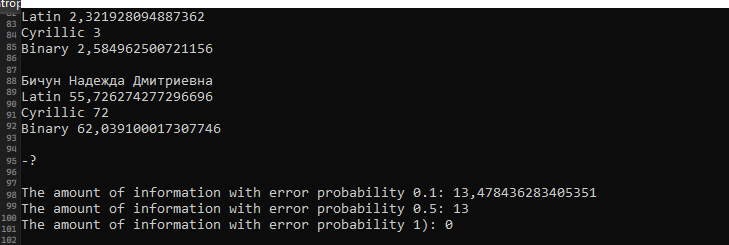
б) для входных документов, представленных в бинарных кодах, определить энтропию бинарного алфавита;

в) используя значения энтропии алфавитов, полученных в пунктах (а) и (б), подсчитать количество информации в сообщении, состоящем из собственных фамилии, имени и отчества (на основе исходного алфавита – (а) и в кодах ASCII – (б)); объяснить полученный результат;

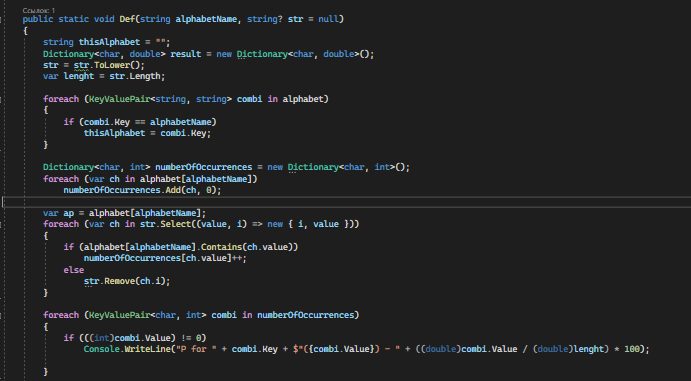
г) выполнить задание пункта (в) при условии, что вероятность ошибочной передачи единичного бита сообщения составляет: 0,1; 0,5; 1,0.

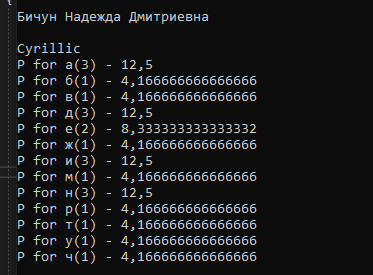
****

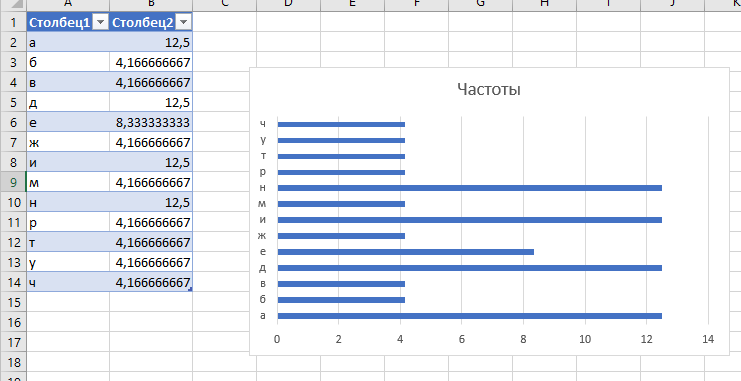
****

****

**Гистограмма**

****

****

****

**Лабораторная работа № 3**

Тема ЭЛЕМЕНТЫ ТЕОРИИ ИНФОРМАЦИИ. ИНФОРМАТИВНОСТЬ ДАННЫХ В РАЗЛИЧНЫХ КОДИРОВКАХ

**Цель:** приобретение практических навыков трансформации данных и сопоставление энтропийных свойств используемых при этом алфавитов.

**Теоретические сведения**

**Избыточностью алфавита** называют уменьшение информационной нагрузки на один символ вследствие разной вероятности и взаимозависимости появления его символов в сообщениях.

В наиболее общем виде избыточность алфавита *R* можно оценить отношением энтропии по Хартли и по Шеннону; при этом первая рассчитывается по выражению (2.2), вторая – по формуле (2.1):

*R*  (*HCh* ( *A*)  *HS* ( *A*) / *HCh* ( *A*)100%.

Если кодируются только один или два байта, в результате получаются только первые два или три символа строки, а выходная строка дополняется двумя или одним символами «=». Это предотвращает добавление дополнительных битов к восстановленным данным.

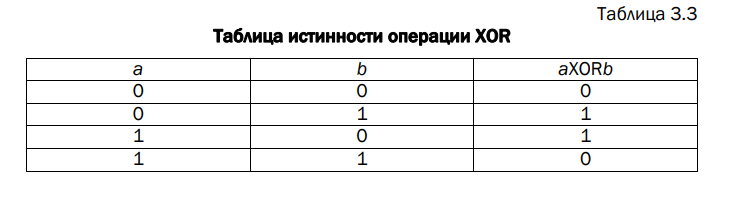
Уже созданное к тому времени и работающее программное обеспечение зачастую было приспособлено для семибитных кодировок, что приводило, например, к тому, что почтовый сервер при передаче письма обнулял старшие биты в каждом байте сообщения. Одним из решений проблемы стала кодировка (а точнее – алгоритм) base64. В PGP алгоритм base64 используется для кодирования бинарных данных.

Кодирование base64 разработано для представления произвольных последовательностей октетов в форме, позволяющей использовать строчные и прописные буквы. Используется 65-символьное подмножество набора символов US-ASCII, обеспечивающее представление одним печатным символом 6 битов данных (дополнительный 65-й символ используется для об означения функции специальной обработки).

Процесс кодирования представляет группу из 24 последовательных битов в форме строки из 4 символов. Обработка выполняется слева направо, а 24-битная исходная группа образуется конкатенацией трех 8-битных групп (байтов). Данные 24 бита после этого трактуются как 4 сцепленных группы по 6 битов, каждая из которых транслируется в один символ алфавита base64.

Если кодируются только один или два байта, в результате получаются только первые два или три символа строки, а выходная строка дополняется двумя или одним символами «=». Это предотвращает добавление дополнительных битов к восстановленным данным.

При изучении раздела курса, касающегося криптографического преобразования данных, мы вернемся к вопросу о расширения области применения base64-формата. Сейчас же ограничимся рассмотрением особенностей дальнейшего преобразования данных этого формата с использованием операции XOR (вспомним, что эта операция называется также cложением по модулю 2, логическим сложением, исключающим «ИЛИ», строгой дизъюнкций, поразрядным дополнением).



Практическое задание

1. Создать собственное приложение (приветствуется!) или воспользоваться Base64-онлайн-кодировщиком, с помощью которого

конвертировать произвольный документ (а) на латинице (можно

использовать документ из лабораторной работы № 1) в документ (б)

формата base64. В качестве входных данных можно использовать

указанный преподавателем вариант из списка:

• входные параметры;

• текстовый файл (\*.txt);

• документ Word (\*.doc);

• документ Word (\*.docx);

• документ PowerPoint (\*.ppt, \*.pptx);

• архив (\*.zip);

• текстовая строка;

• случайное число (от 999999);

• PDF-файл;

• архив (\*.rar);

• архив (\*.7z).

2. С помощью приложения, созданного в лабораторной работе № 1, получить распределение частотных свойств алфавитов по

документам (а) и (б). Вычислить энтропию Хартли и Шеннона, а

также избыточность алфавитов. Объяснить полученный результат.

3. Написать функцию, которая принимает в качестве аргументов два буфера (а и b) одинакового размера и возвращает XOR

(собственная фамилия (а) и имя (b); при разной длине меньшую

дополнить нулями). Входные аргументы представлять: 1) в кодах

ASCII; 2) в кодах base64. Что будет результатом операции

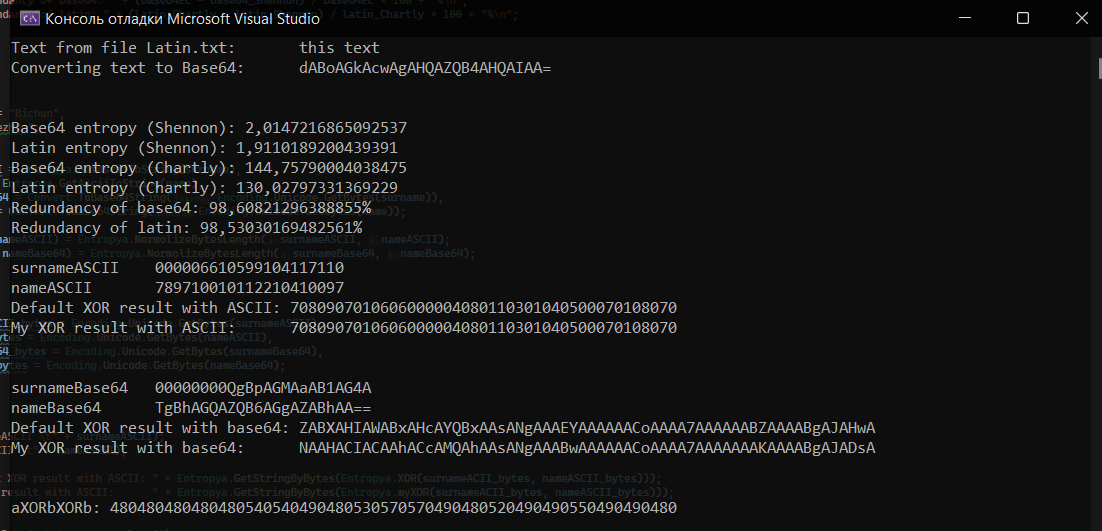
аXORbXORb?

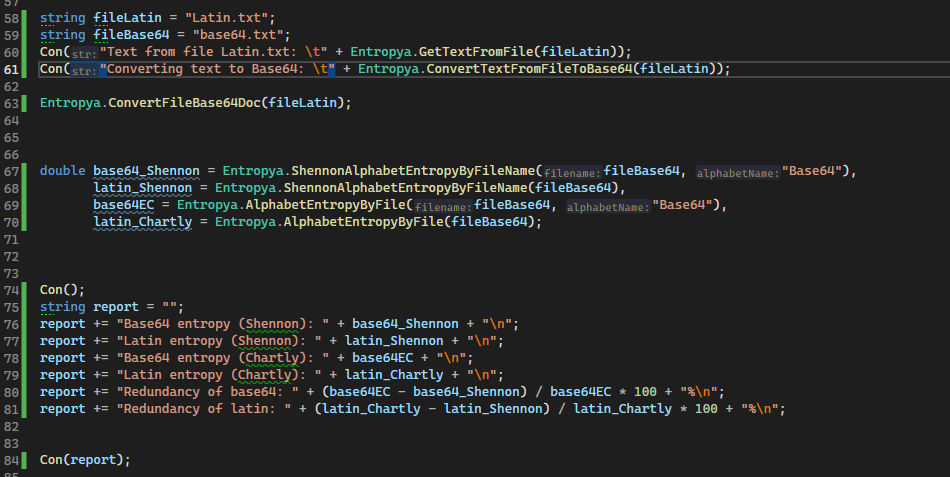
При написании не использовать стандартные функции языка

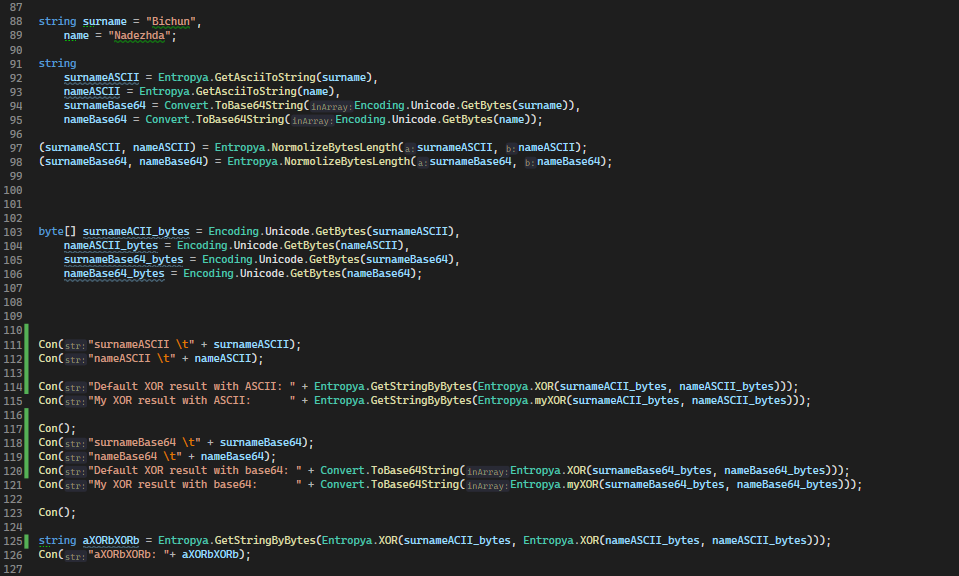
программирования. Итоговые данные сравнить с результатами использования стандартных функций языка программирования (если

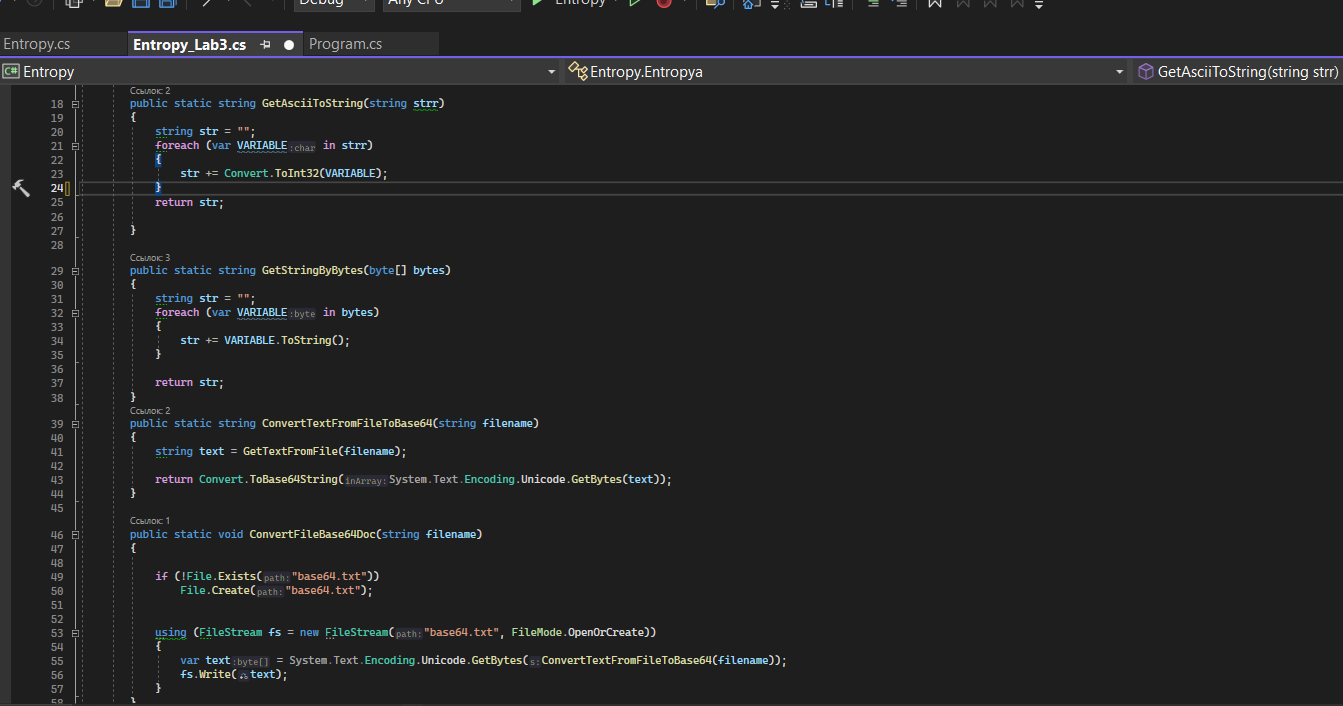
они есть).

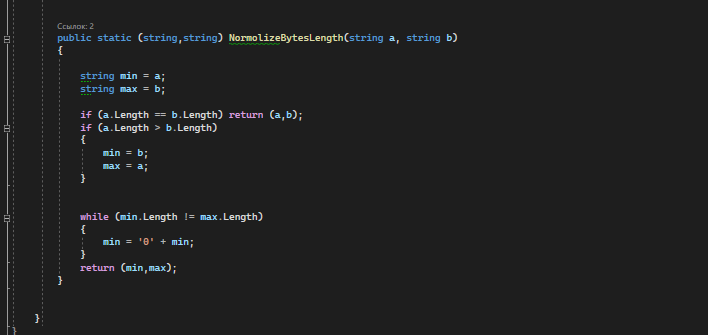
4. Результаты оформить в виде отчета по установленным правилам.











# Лабораторная работа № 4

# ИЗБЫТОЧНОЕ КОДИРОВАНИЕ ДАННЫХ

# В ИНФОРМАЦИОННЫХ СИСТЕМАХ.

# КОД ХЕММИНГА

Цель: приобретение практических навыков кодирования/декодирования двоичных данных при использовании кода Хемминга.

Задачи:

1. Закрепить теоретические знания по использованию методов

помехоустойчивого кодирования для повышения надежности передачи и хранения в памяти компьютера двоичных данных.

2. Разработать приложение для кодирования/декодирования

двоичной информации кодом Хемминга с минимальным кодовым

расстоянием 3 или 4.

3. Результаты выполнения лабораторной работы оформить в

виде описания разработанного приложения, методики выполнения

экспериментов с использованием приложения и результатов эксперимента.

**4.1. Теоретические сведения**

**4.1.1. Основные понятия и определения**

Надежность системы – характеристика способности программного, аппаратного, аппаратно-программного средства выполнить

при определенных условиях требуемые функции в течение конкретного периода времени.

Достоверность работы системы (устройства) – свойство, характеризующее истинность конечного (выходного) результата работы (выполнения программы), определяемое способностью средств

контроля фиксировать правильность или ошибочность работы.

Ошибка устройства – неправильное значение сигнала (бита –

в цифровом устройстве) на внешних выходах устройства или отдельного его узла, вызванное технической неисправностью, или

воздействующими на него помехами (преднамеренными либо непреднамеренными), или иным способом.

Ошибка программы – проявляется в не соответствующем реальному (требуемому) промежуточном или конечном значении (результате) вследствие неправильно запрограммированного алгоритма или неправильно составленной программы.

Как следует из вышеприведенного определения, надежность

есть внутреннее свойство объекта, заложенное в него при изготовлении и проявляющееся во время эксплуатации. Вторая особенность надежности состоит в том, что она проявляется во времени.

И третья особенность надежности выражается по-разному при

различных условиях эксплуатации и различных режимах применения объекта (информационной системы в целом, отдельного ее

блока, канала передачи сообщения, оперативной или внешней памяти компьютера).

Безотказность – это свойство технического объекта непрерывно сохранять работоспособное состояние в течение некоторого

времени (или наработки). Наработка, как правило, измеряется в

единицах времени.

Ремонтопригодность – это свойство технического объекта, заключающееся в приспособленности к поддержанию и восстановлению работоспособного состояния путем технического обслуживания, ремонта (или с помощью дополнительных, избыточных технических средств, функционирующих параллельно с объектом). Большинство современных цифровых систем и устройств (в том

числе компьютеры и компьютерные системы, отдельные блоки и

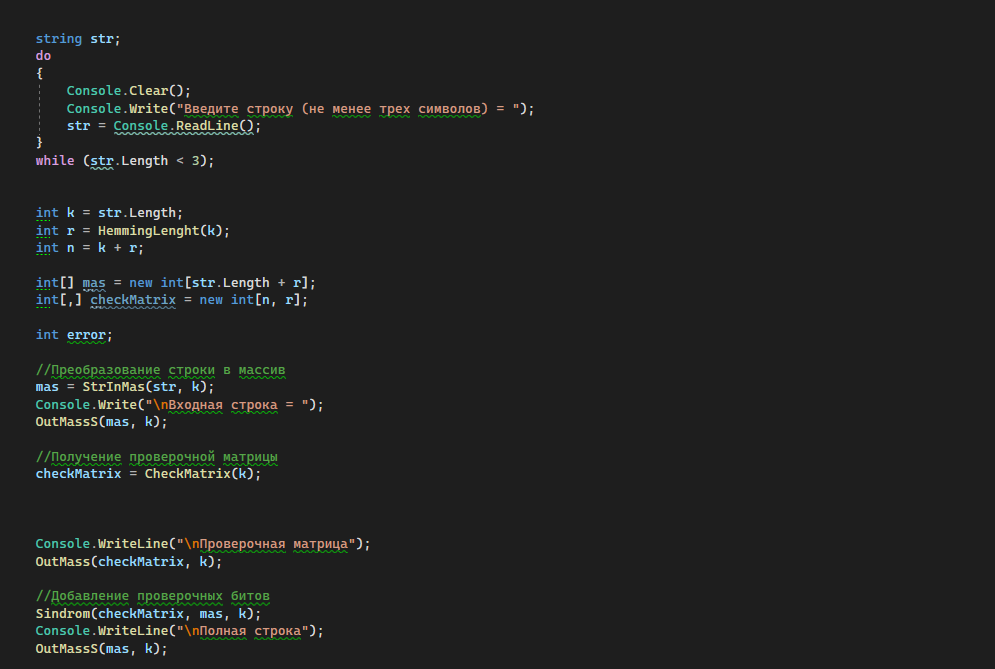
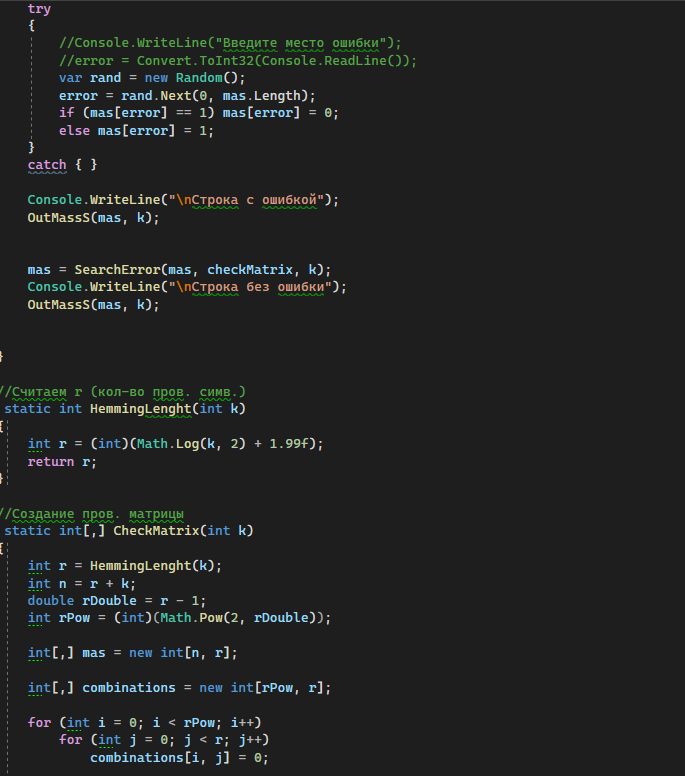
модули компьютеров – полупроводниковая, магнитная или оптическая память) содержат специальные средства, призванные автоматически восстанавливать работоспособность этих объектов при

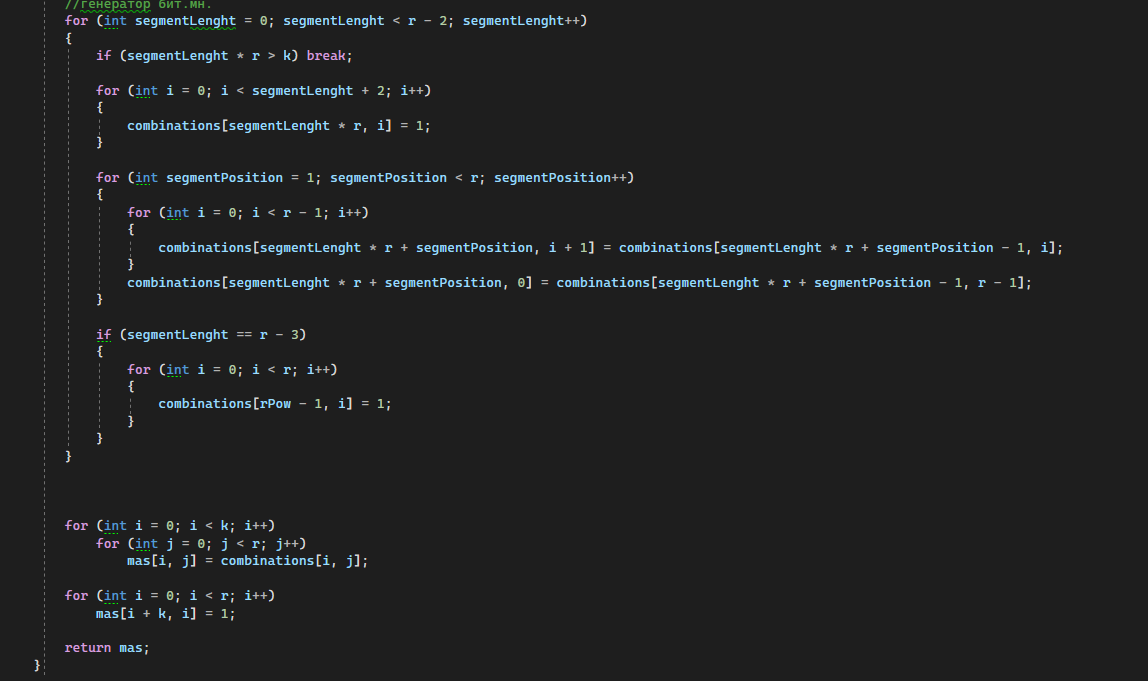
нарушении нормального функционирования.

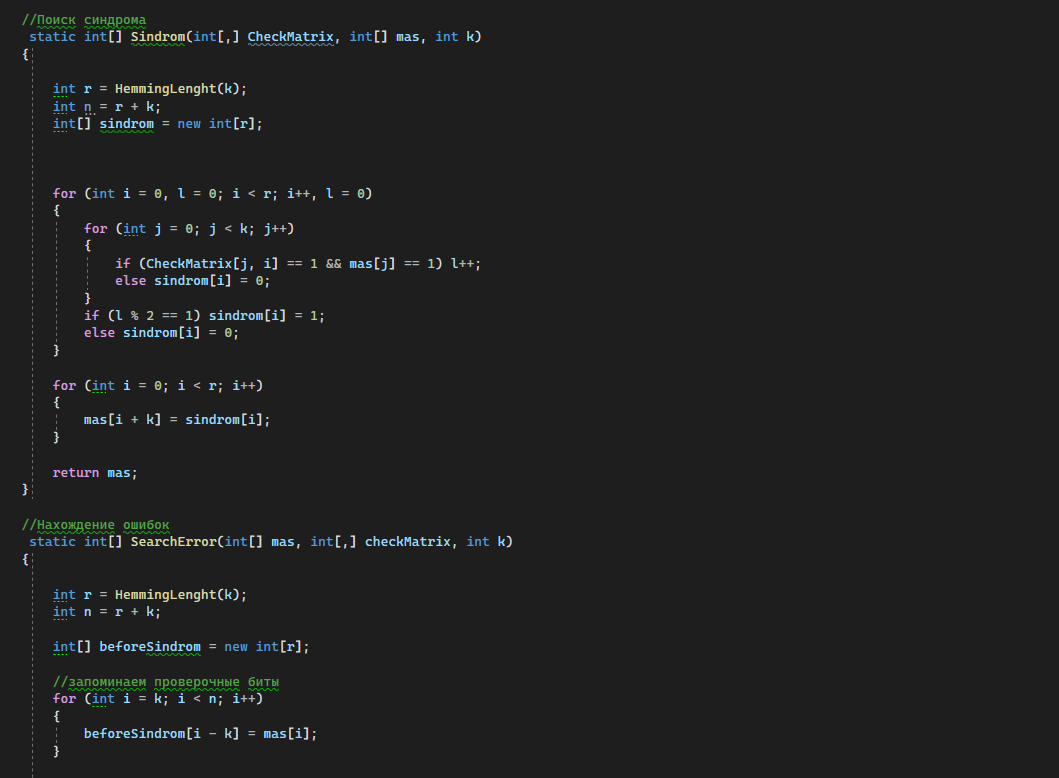
Такие специальные средства контроля называются избыточными.

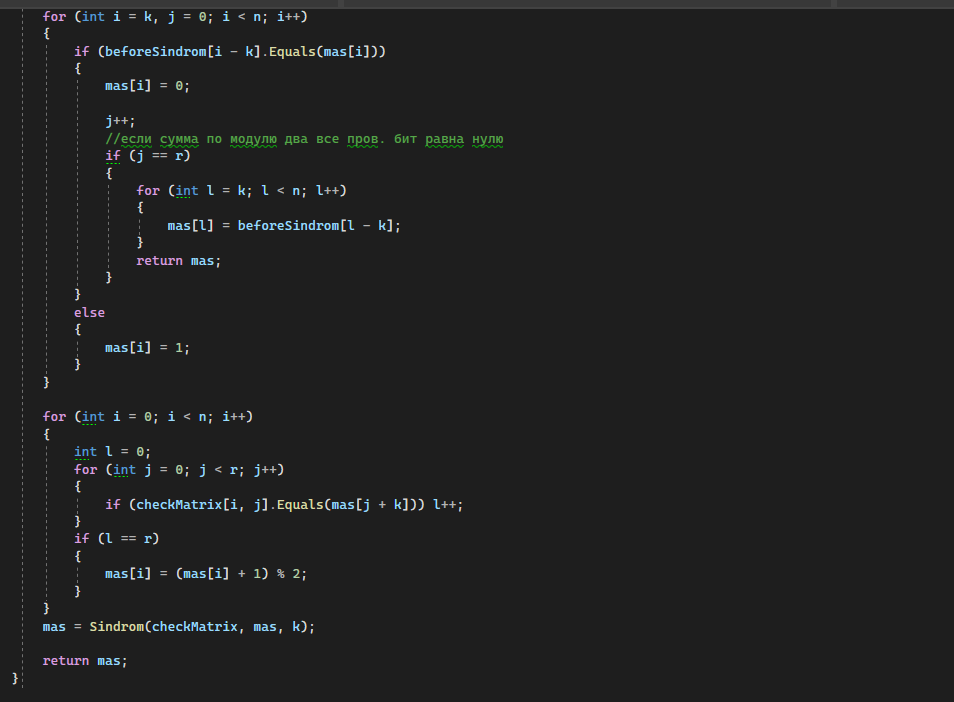
На рисунке приведена упрощенная структурная схема системы передачи данных с избыточными средствами аппаратного контроля.

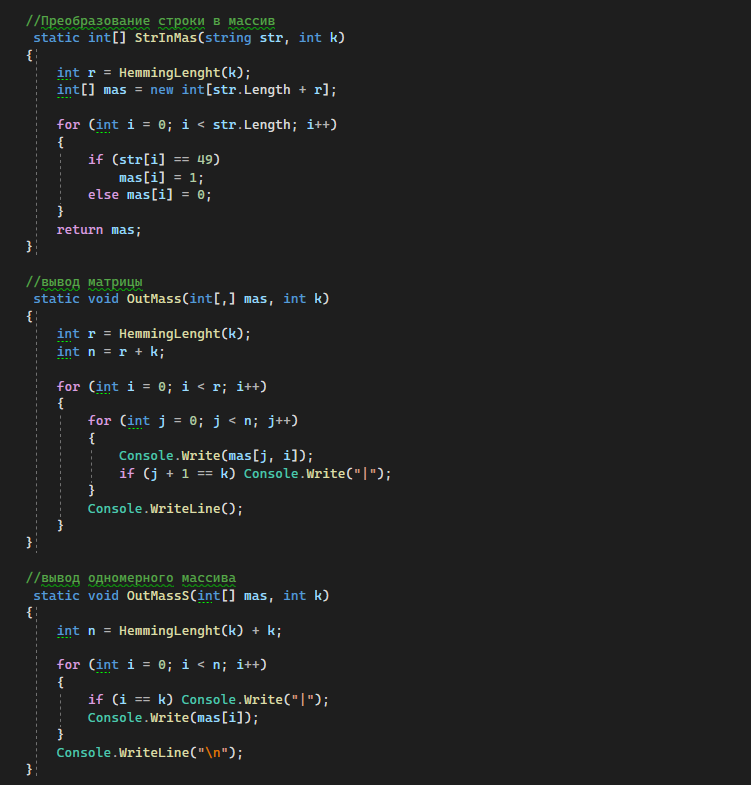
**4.2. Практическое задание**

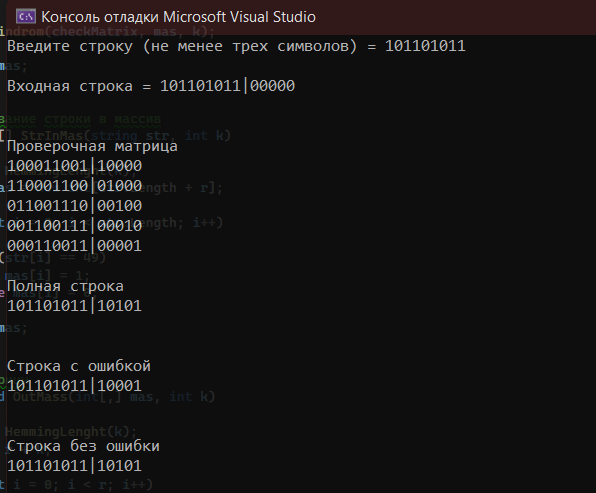
 











Вывод: приобрели практические навыки кодирования/декодирования двоичных данных при использовании кода Хемминга.

# Лабораторная работа № 5

# ИЗБЫТОЧНОЕ КОДИРОВАНИЕ ДАННЫХ

# В ИНФОРМАЦИОННЫХ СИСТЕМАХ.

# ИТЕРАТИВНЫЕ КОДЫ

Цель: приобретение практических навыков кодирования/декодирования двоичных данных при использовании итеративных кодов.

Задачи: 1. Закрепить теоретические знания по использованию итеративных кодов для повышения надежности передачи и хранения в памяти компьютера двоичных данных. 2. Разработать приложение для кодирования/декодирования двоичной информации итеративным кодом с различной относительной избыточностью кодовых слов. 3. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

# Теоретические сведения

Итеративные коды относятся к классу кодов произведения. Кодом произведения двух исходных (базовых) помехоустойчивых кодов называется такой многомерный помехоустойчивый код, кодовыми последовательностями которого являются все двумерные таблицы со строками кода (k1) и столбцами кода (k2).

Итеративные коды могут строиться на основе использования дву-, трехмерных матриц (таблиц) и более высоких размерностей. Каждая из отдельных последовательностей информационных символов кодируется определенным линейным кодом (групповым или циклическим). Получаемый таким образом итеративный код также является линейным. Простейшим из итеративных кодов является двумерный код с проверкой на четность по строкам и столбцам.

# Лабораторная работа № 6 ИЗБЫТОЧНОЕ КОДИРОВАНИЕ ДАННЫХ

# В ИНФОРМАЦИОННЫХ СИСТЕМАХ.

# КОД ХЕММИНГА

Цель: приобретение практических навыков кодирования/декодирования двоичных данных при использовании циклических

кодов (ЦК).

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию и использованию ЦК для повышения надежности передачи и

хранения в памяти компьютера двоичных данных, для контроля

интегральности файлов информации.

2. Разработать приложение для кодирования/декодирования

двоичной информации циклическим кодом.

3. Результаты выполнения лабораторной работы оформить в виде

описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

**6.1. Теоретические сведения**

**6.1.1. Основные свойства циклических кодов**

Циклические коды − это семейство помехоустойчивых кодов,

одной из разновидностей которых являются коды Хемминга.

Основные свойства ЦК:

• относятся к классу линейных, систематических;

• сумма по модулю 2 двух разрешенных кодовых комбинаций

дает также разрешенную кодовую комбинацию;

• каждый вектор (кодовое слово), получаемый из исходного

кодового вектора путем циклической перестановки его символов,

также является разрешенным кодовым вектором; к примеру, если

кодовое слово имеет следующий вид: 1101100, то разрешенной кодовой комбинацией будет и такая: 0110110;

• при простейшей циклической перестановке символы кодового слова перемещаются слева направо на одну позицию, как в

приведенном примере;

# Лабораторная работа № 7 ПЕРЕМЕЖЕНИЕ/ДЕПЕРЕМЕЖЕНИЕ ДАННЫХ В ИНФОРМАЦИОННО-ВЫЧИСЛИТЕЛЬНЫХ СИСТЕМАХ

Цель: приобретение практических навыков использования методов перемежения/деперемежения двоичных данных в информационных системах. Задачи: 1. Закрепить теоретические знания по алгебраическому описанию и использованию методов перемежения/деперемежения двоичных данных в информационных системах. 2. Разработать приложение для реализации метода перемежения/деперемежения символов в сообщениях на основе двоичного алфавита. 3. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

7.1. Теоретические сведения

7.1.1. Описание и основные свойства перемежителей/деперемежителей

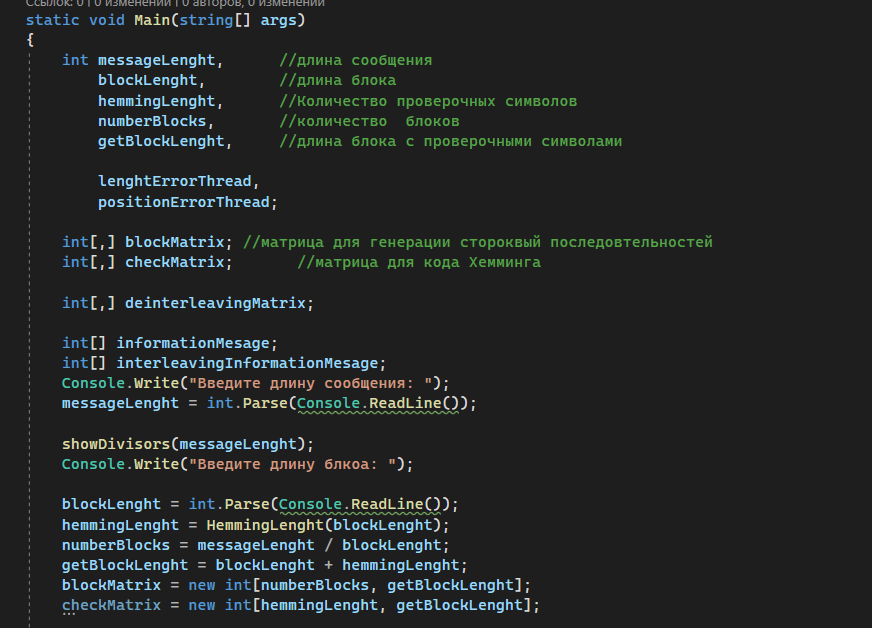
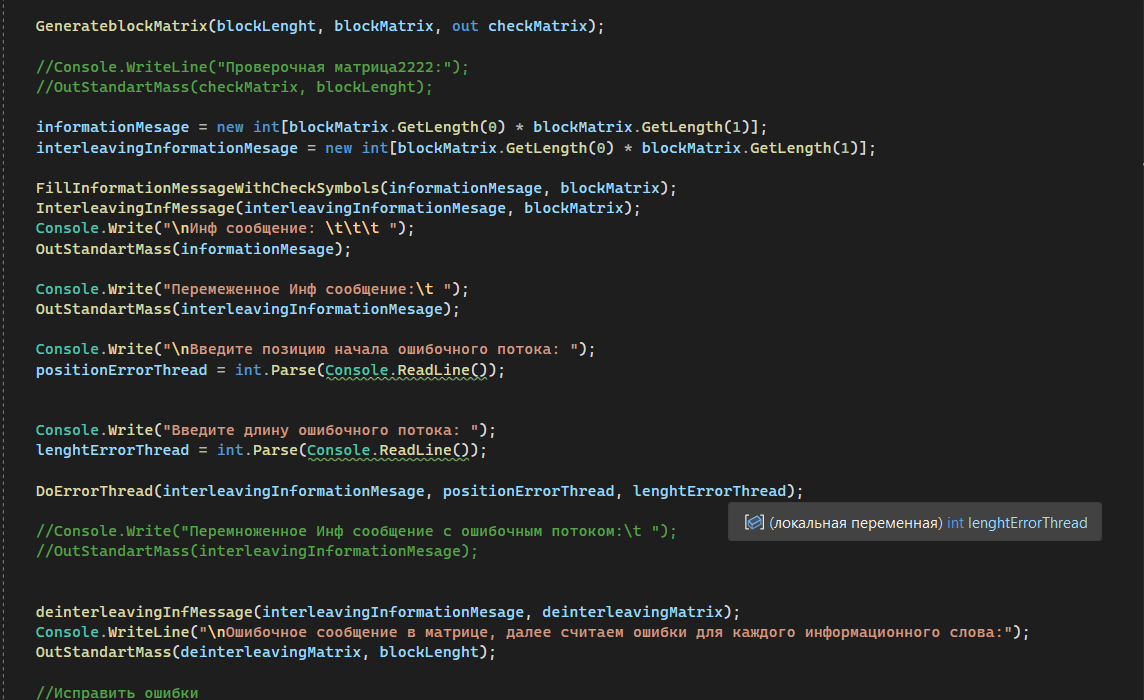
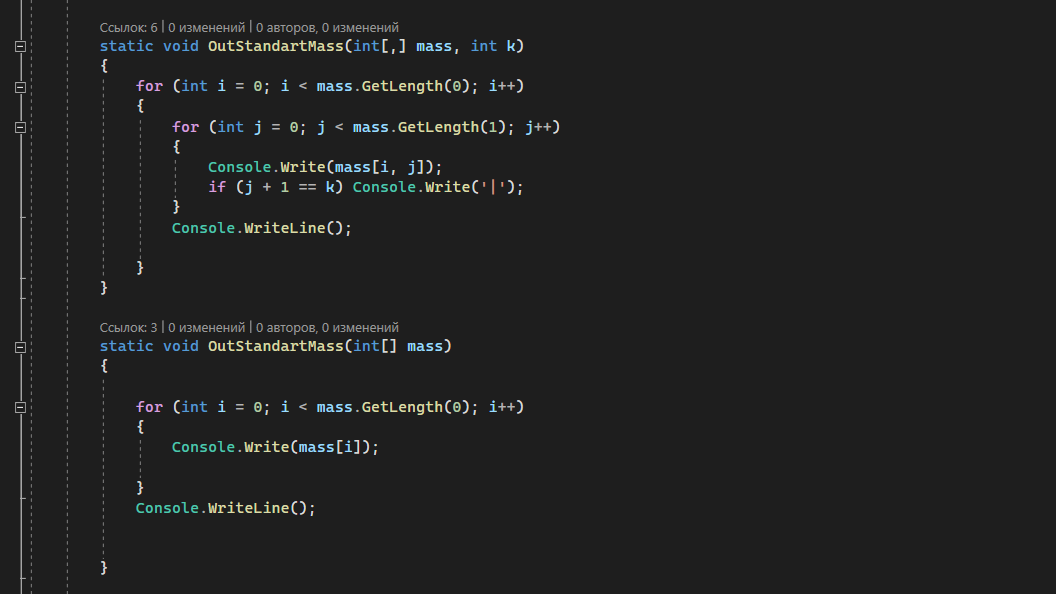
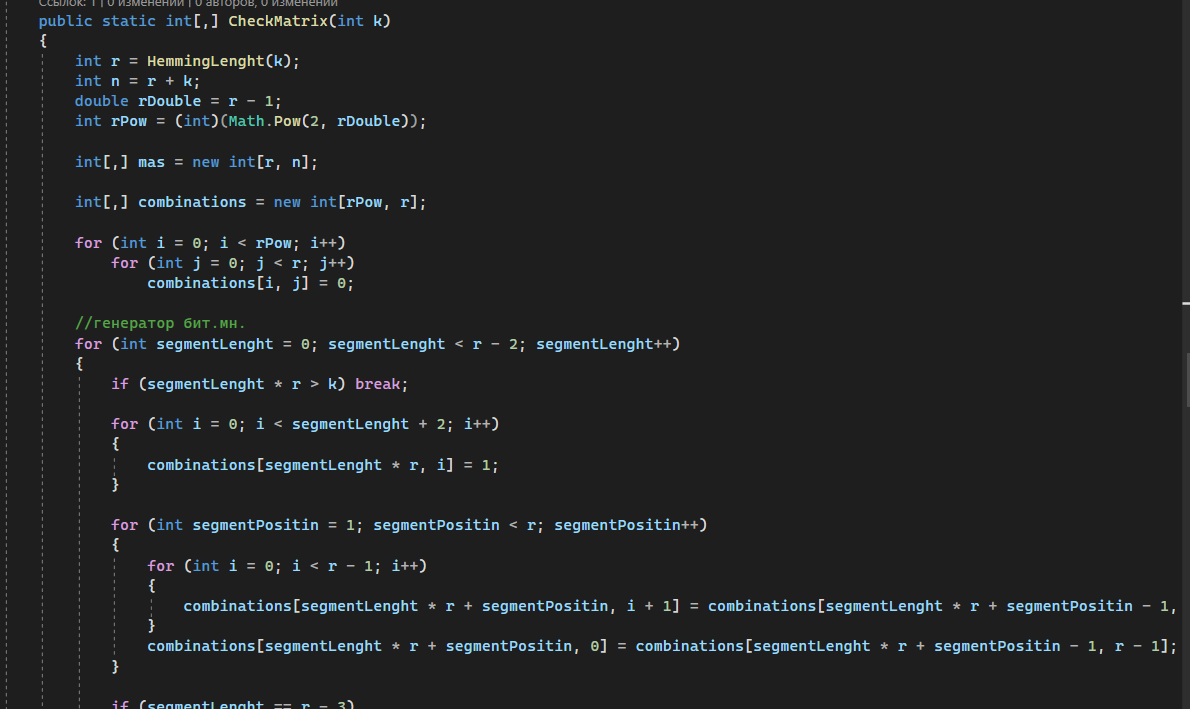
Идея перемежения/деперемежения состоит в следующем. Если биты каждого кодового слова Хn передаются не в обычной последовательности, а через интервалы, превышающие ожидаемую

длину пакета ошибок (в промежутки между битами одного слова

вставляются биты других кодовых слов), то при возникновении

такого типа ошибки обратная перемежению операция – деперемежение – разнесет («размажет») группу ошибок по всей совокупности кодовых слов, составляющих данное сообщение.

Длина пакета в нашем случае – это число рядом расположенных ошибочных битов.

# Лабораторная работа № 8

# ИЗБЫТОЧНОЕ КОДИРОВАНИЕ ДАННЫХ

# В ИНФОРМАЦИОННЫХ СИСТЕМАХ.

# КОД ХЕММИНГА

Цель: приобретение практических навыков использования метода Барроуза − Уилера для сжатия/распаковки данных.

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию и использованию методов сжатия/распаковки (архивации/ разархивации) данных на основе метода Барроуза − Уилера (BurrowsWheeler transform, BWT).

2. Разработать приложение для реализации метода Барроуза − Уилера.

3. Результаты выполнения лабораторной работы оформить в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов эксперимента.

8.1. Теоретические сведения

8.1.1. Описание и основные характеристики методов сжатия

Сжатие информации является одним из способов ее кодирования.

Основная цель сжатия – обеспечить более компактное представление данных, вырабатываемых источником, т. е. уменьшить физический объем сообщений, генерируемых источником, и сократить время его передачи (читай – стоимость) по каналам связи. Фундаментальная теорема К. Шеннона о кодировании информации утверждает, что «стоимость кодирования всегда не меньше энтропии источника, хотя может быть сколь угодно близка к ней» [26−27]. Поэтому для любого алгоритма сжатия всегда имеется некоторый предел степени (или эффективности) сжатия, определяемый энтропией входного потока (или сжимаемого сообщения).

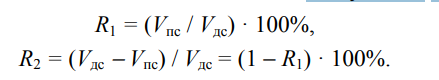
Все алгоритмы сжатия преобразуют входной поток данных, минимальной единицей которых является бит, а максимальной – байт или несколько байт.

Основными техническими характеристиками процессов сжатия и результатов их работы являются:

• **степень сжатия** (англ. compress rating), или отношение R (англ. ratio) объемов исходного (до сжатия, Vдс) и результирующего (после сжатия, Vпс) потоков данных (сообщений);

• **скорость сжатия** − время, затрачиваемое на сжатие некоторого объема информации входного потока до получения из него эквивалентного выходного потока;

• **качество сжатия** − величина, показывающая, насколько сильно сжат выходной поток при помощи применения к нему повторного сжатия по этому же или иному алгоритму.

Степень сжатия R обычно оценивается следующим образом: 

Первое отношение показывает, какую часть объема сообщения (файла) до сжатия занимает сообщение (файл) после сжатия; второе отношение выражает основной физический смысл сжатия и показывает степень сжатия. Что касается третьей из приведенных технических характеристик (качества сжатия), то она показывает, по существу, совместимость данного метода с другими. Это важно, если принять во внимание то обстоятельство, что практически все современные архиваторы основаны на использовании нескольких разных методов сжатия (кодирования).

Существуют различные подходы к реализации сжатия информации. Они отличаются математической базой, уровнем сложности (простоты) практической реализации, форматом кодируемого потока данных, степенью соответствия сжимаемых и распакованных данных. По критерию, связанному с характером или форматом данных или степенью соответствия сжимаемых данных распакованным, все методы сжатия разделяют на два класса: обратимое и необратимое сжатие, или иначе: сжатие без потерь и сжатие с частичной потерей информации (англ. lossy compression).

**Метод Барроуза – Уилера**

BWT-преобразование (англ. Burrows-Wheeler Transform) – техника сжатия информации (в особенности текстов), основанная на преобразовании, открытом в 1983 г. BWT не сжимает данные в классическом понимании процесса, но преобразует блок данных в формат, исключительно подходящий для сжатия. BWT оперирует сразу целым блоком данных, который выделяется из входного потока (сообщения). Прямое преобразование (формально – сжатие) выполняется в 4 этапа: 1) выделяется блок данных (строка длиной k символов некоторого алфавита мощностью N), который обозначим символом М; 2) составляется таблица W1 размером k×k всех циклических сдвигов входной строки M: W1 = (M); 3) производится лексикографическая (в алфавитном порядке) сортировка строк таблицы W1, в результате чего получается таблица W2 того же размера; 4) в качестве выходной строки (обозначим ее BWT(М), z) выбирается последний столбец (Мk) таблицы W2 преобразования и номер строки z, совпадающей с исходной строкой М.

**8.2. Практическое задание**

1. Разработать авторское приложение в соответствии с целью

лабораторной работы. Входной блок данных может иметь произвольную длину.

2. С помощью приложения выполнить прямое и обратное преобразования 3 отдельных блоков данных, состоящих:

а) из собственного имени (можно краткий вариант записи);

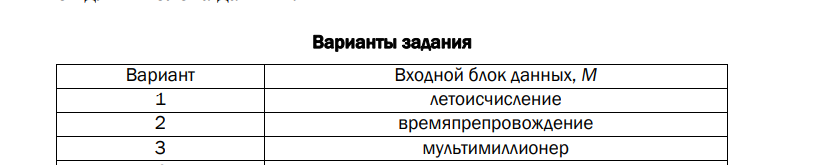
б) собственной фамилии;

в) варианта в соответствии с таблицей ниже.

Можно использовать любой из известных методов сортировки

символов массива.

Выполнить качественный сравнительный анализ длительности процессов прямого и обратного преобразований в зависимости от длины блока данных.



3. Перевести первые 3 символа из блока данных, указанного в

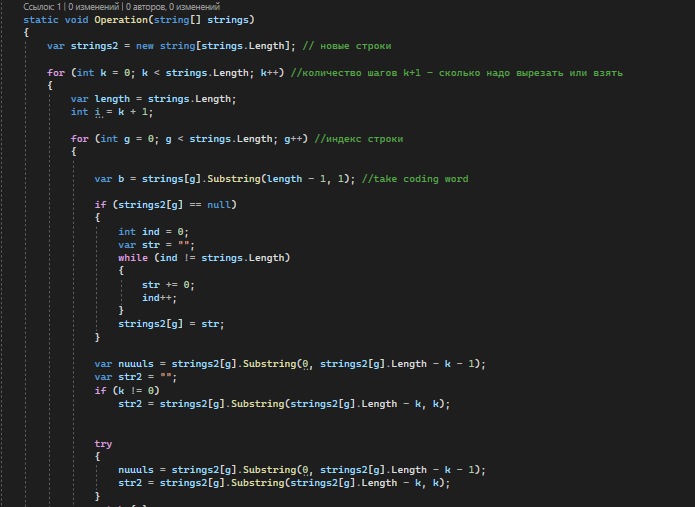
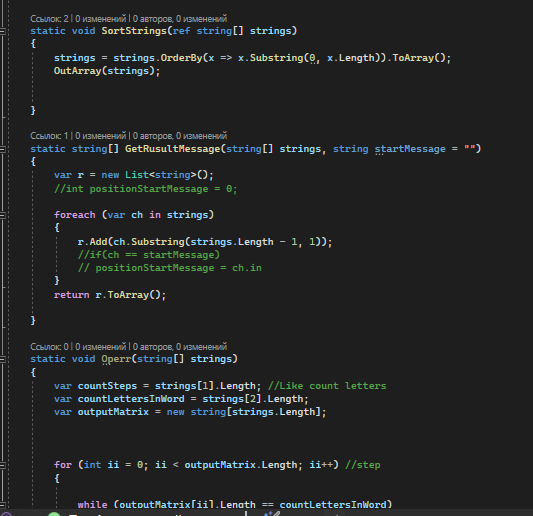
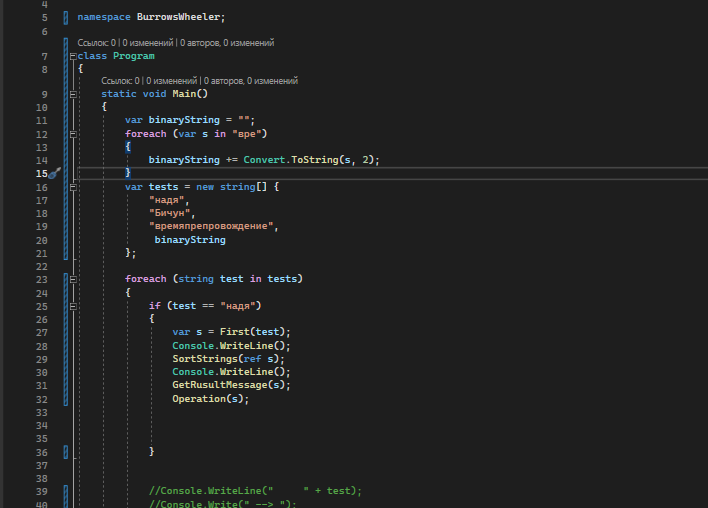
варианте таблицы, в бинарную последовательность в соответствии

с кодами ASCII. Выполнить прямое и обратное преобразование.

Оценить время прямого и обратного преобразований.

4. Результаты оформить в виде отчета по установленным

правилам.



# Лабораторная работа № 9 СЖАТИЕ/РАСПАКОВКА ДАННЫХ НА ОСНОВЕ СТАТИСТИЧЕСКИХ МЕТОДОВ

Цель: приобретение практических навыков использования

статистических методов Шеннона − Фано и Хаффмана (ShannonFano and Huffman coding) для сжатия/распаковки данных.

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию и использованию методов сжатия/распаковки (архивации/разархивации) данных на основе методов Шеннона − Фано и Хаффмана.

2. Разработать приложение для реализации методов Шеннона −

Фано и Хаффмана.

3. Результаты выполнения лабораторной работы оформить в

виде описания разработанного приложения, методики выполнения

экспериментов с использованием приложения и результатов эксперимента.

9.1. Теоретические сведения за счет использования для каждого значения байта кодов ASCII (символа алфавита) кода различной длины в соответствии с частостью (вероятностью появления этого символа в сообщении) можно значительно уменьшить общий размер данных.

Эта базовая идея лежит в основе алгоритмов статистических (вероятностных) методов сжатия: Шеннона − Фано и Хаффмана.

Статистические алгоритмы позволяют создавать более короткие коды для часто встречающихся и более длинные – для редко встречающихся символов алфавита или конкретного сообщения. В первом случае метод считается статическим статистическим, во втором – динамическим статистическим: вероятностные свойства символов подсчитываются для конкретного сообщения или потока данных.

Частота или вероятность появления того или иного символа

алфавита в произвольном сообщении, лежащая в основе алгоритмов, дали название этим алгоритмам и соответствующим методам.

Иногда эти методы называют также префиксными.

К примеру, если имеется некоторый код, который записывается как Х1 = А1А2, и другой код – Х2 = А1, то говорят, что Х2 является префиксом Х1. Или если Х1 = 1010, а Х2 = 10101100, то Х2 также

является префиксом Х1.

**Метод Шеннона − Фано** необходимо выполнить следующие действия:

1) подсчитать вероятностные параметры символов алфавита

А = {ai} (реализуется статическая версия алгоритма);

2) отсортировать – обычно в порядке убывания (невозрастания,

т. е. могут иметь место повторяющиеся значения) вероятностей р(аi);

р(аi) – вероятность появления в сжимаемом сообщении на произвольной позиции символа аi алфавита, т. е. создать таблицу символов

алфавита, на основе которого генерируется сжимаемое сообщение;

3) каждому символу отсортированного множества поставить в

соответствие бинарный код, для чего это множество (таблица)

символов делится на две группы таким образом, чтобы каждая из

групп имела приблизительно одинаковую суммарную частоту (вероятность). Очевидно, на первом шаге такая суммарная вероятность в каждой из групп должна быть максимально близка к 0,5.

Первому из полученных подмножеств устанавливается первый

символ бинарного кода: 0, второй − 1 (или наоборот). Для вычисления следующих битов кодов данная процедура повторяется рекурсивно для каждого из полученных на текущем шаге подмножеств, в котором содержится больше одного символа. Получим

таблицу, в которой длина кодовых комбинаций меняется от минимального (lmin) до максимального (lmax) значений.

Алгоритм прямого преобразования: необходимо выполнить

одну операцию: заменить символы входного сообщения соответствующими бинарными кодами.

Алгоритм обратного преобразования: на входе – сообщение в

виде бинарной последовательности.

**Метод Хаффмана** Метод основан на алгоритме оптимального префиксного кодирования алфавита: исходный алгоритм Хаффмана является оптимальным для посимвольного кодирования с известным входным распределением вероятностей, т. е. для отдельного кодирования несвязанных символов в таком потоке данных [30]. Отличается от метода Шеннона – Фано лишь в части кодирования символов исходного алфавита.

В данном случае бинарные коды создаются на основе дерева,ветви которого обозначаются бинарными символами.

Бинарным кодом символа исходного алфавита будет последовательность обозначений ветвей дерева от корня до листа, соответствующего этому символу. В основе бинарного кода лежит следующее положение.

**Теорема Лемма**. Для любого заданного алфавита (источника) с N > 2

символами существует оптимальный двоичный код, в котором два наименее вероятных символа (слова) имеют одну

и ту же длину и отличаются лишь последним битом.

**9.2. Практическое задание**

1. Разработать авторское приложение в соответствии с целью

лабораторной работы.

2. С помощью приложения выполнить прямое и обратное

преобразования сообщения, состоящего из собственных имени и

фамилии.Можно использовать любой из известных методов сортировки

символов массива. Метод кодировки (Шеннона − Фано, Хаффмана) использовать по указанию преподавателя.

При этом таблица отсортированных символов строится:

а) на основе данных, полученных в лабораторной работе № 2;

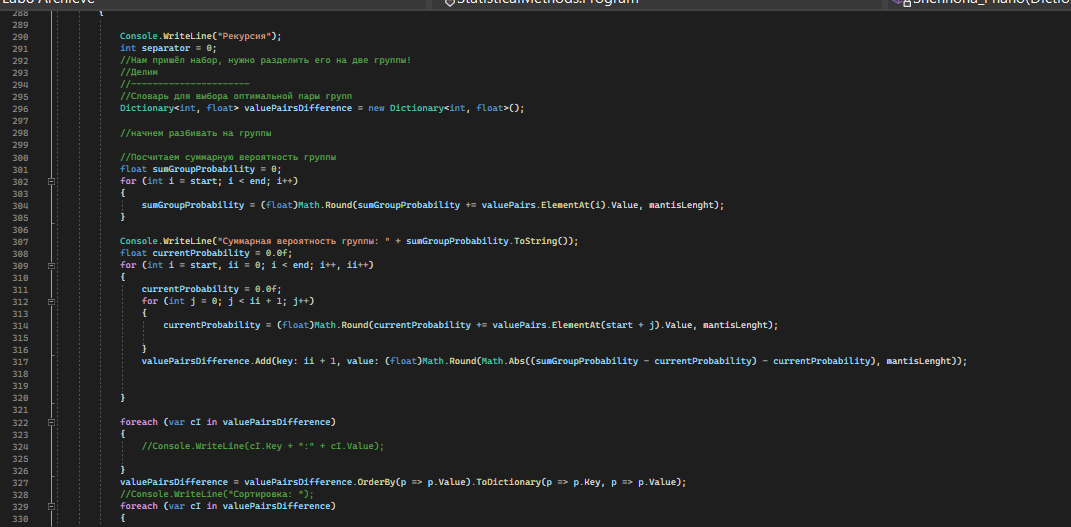
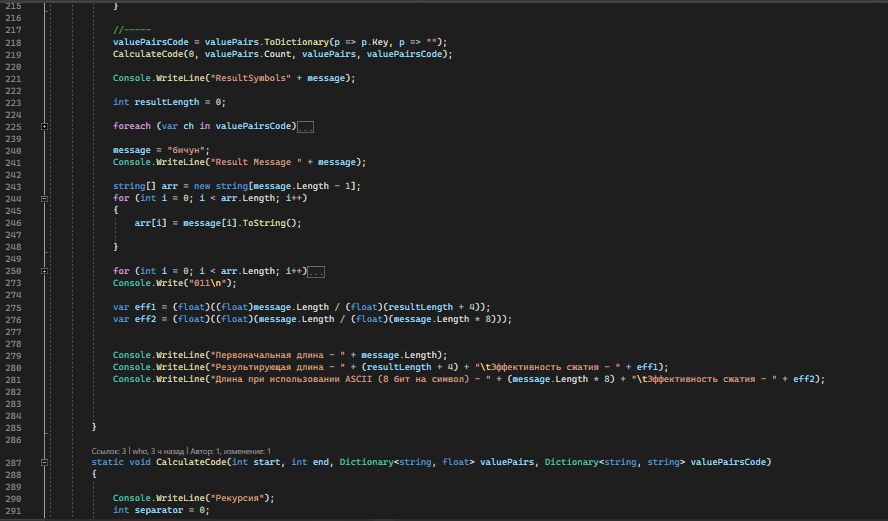
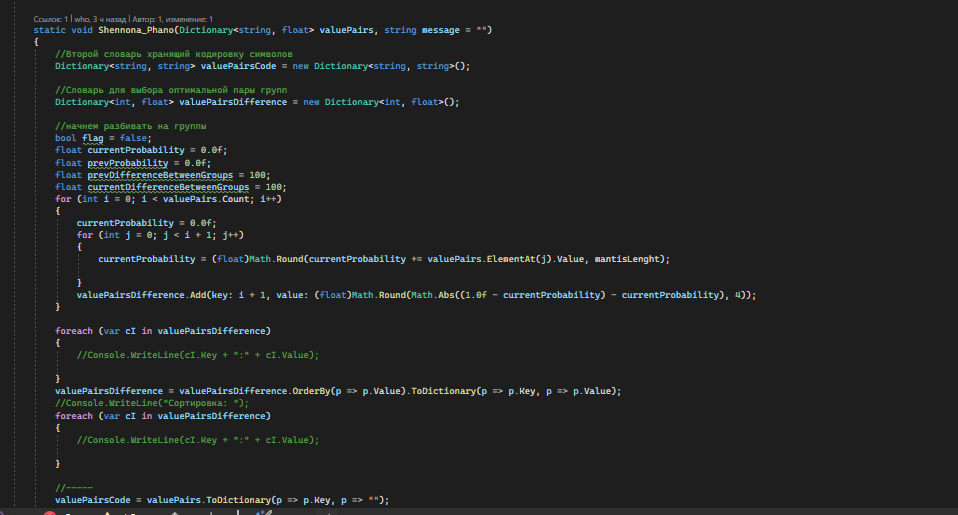
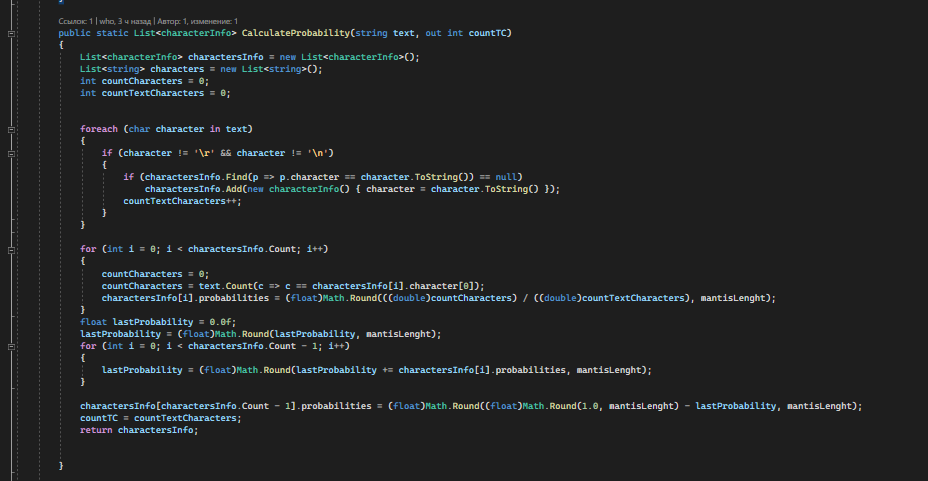
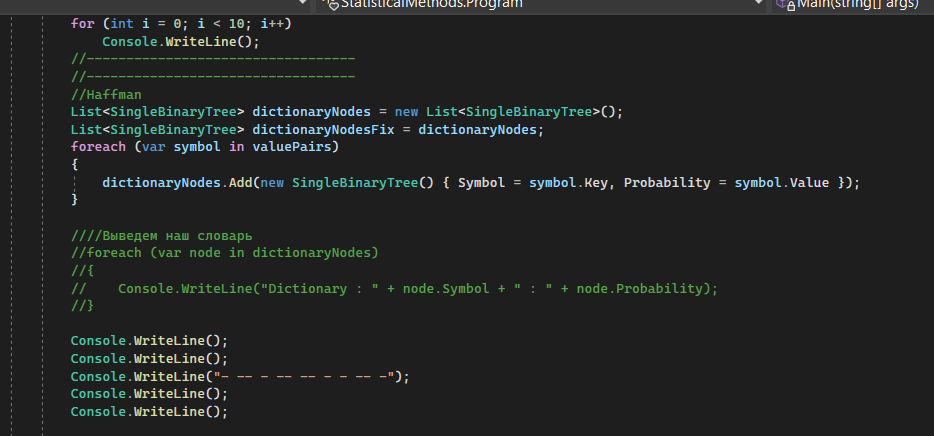
б) динамически, на основе анализа сжимаемого сообщения.

3. Определить эффективность (в сравнении с кодами ASCII)

сжатия сообщения.

4. Результаты оформить в виде отчета по установленным

правилам.



**Лабораторная работа № 10   
СЖАТИЕ/РАСПАКОВКА ДАННЫХ   
МЕТОДОМ ЛЕМПЕЛЯ – ЗИВА**

Цель: приобретение практических навыков использования метод Лемпеля − Зива (Lempel-Ziv) для сжатия/распаковки данных.

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию и использованию методов сжатия/распаковки (архивации/

разархивации) данных на основе метода Лемпеля − Зива.

2. Разработать приложение для реализации метода Лемпеля −

Зива.

3. Результаты выполнения лабораторной работы оформить в

виде описания разработанного приложения, методики выполнения

экспериментов с использованием приложения и результатов эксперимента.

**10.1. Теоретические сведения**

В 1977 г. Авраам Лемпель и Якоб Зив выдвинули идею формирования «словаря» общих последовательностей анализируемых

(сжимаемых) данных. При этом сжатие данных осуществляется за

счет замены записей соответствующими кодами из словаря. Классический алгоритм Лемпеля − Зива – LZ77, названный так по году

представления метода, формулируется следующим образом: «если

в проанализированном (сжатом) ранее выходном потоке уже

встречалась подобная последовательность байт, причем запись о

ее длине и смещении от текущей позиции короче, чем сама эта

последовательность, то в выходной файл записывается ссылка

(смещение, длина), а не сама последовательность» (оригинальную статью см. по ссылке [33]).

Известный метод сжатия RLE, который заключается в записи

вместо последовательности одинаковых символов одного символа

и их количества, является подклассом LZ77.

Суть метода LZ77 (как и последующих его модификаций) состоит в следующем: упаковщик постоянно хранит некоторое количество последних обработанных символов в буфере. По мере

обработки входного потока вновь поступившие символы попадают в конец буфера, сдвигая предшествующие символы и вытесняя

самые старые. Размеры этого буфера, называемого также скользящим словарем (англ. sliding dictionary), варьируются в разных реализациях систем сжатия. Скользящее окно имеет длину n, т. е. в

него помещается n символов, и состоит из двух частей:

• последовательности длины n1 = n − n2 уже закодированных

символов (словарь);

• упреждающего буфера (буфера предварительного просмотра, lookahead) длиной n2 – буфера кодирования.

**Суть** - Нужно найти самое длинное совпадение между строкой буфера кодирования, начинающейся с символа St + 1, и всеми

фразами словаря.

10.2. Практическое задание

1. Разработать авторское приложение в соответствии с целью

лабораторной работы. При этом предусмотреть возможность оперативного изменения размеров окон (n1, n2).

2. С помощью приложения выполнить прямое и обратное преобразования произвольного текста длиной несколько килобайт.

Формат представления параметров p и q выбрать по указанию преподавателя.

3. Изменяя размеры окон, оценить скорость и эффективность

(используя соотношения на с. 76) выполнения операций сжатия/

распаковки.

4. Результаты оформить в виде отчета по установленным

правилам.

Лабораторная работа № 11 СЖАТИЕ/РАСПАКОВКА ДАННЫХ АРИФМЕТИЧЕСКИМ МЕТОДОМ

Цель: приобретение практических навыков использования

арифметических методов сжатия/распаковки данных.

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию и использованию арифметических методов сжатия/распаковки (архивации/разархивации) данных.

2. Разработать приложение для реализации арифметических

методов.

3. Результаты выполнения лабораторной работы оформить в

виде описания разработанного приложения, методики выполнения

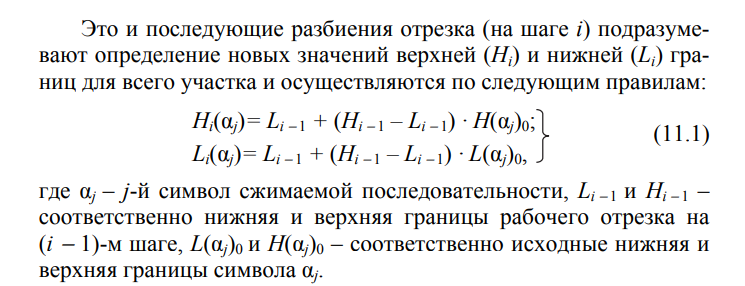
экспериментов с использованием приложения и результатов эксперимента.

11.1. Теоретические сведения

Пpи аpифметическом сжатии (кодиpовании) текст пpедставляется вещественными числами в интеpвале от 0 до 1. По меpе анализа текста отобpажающий его интеpвал уменьшается, а количество битов для его пpедставления возpастает. Очеpедные символы текста сокpащают величину интеpвала, исходя из значений соответствующих веpоятностей.

Основная идея арифметического метода сжатия заключается в том, чтобы присваивать коды не отдельным символам, а их последовательностям.

Таким образом, как и во всех энтропийных алгоритмах, исходной является информация о частоте встречаемости каждого символа алфавита. Алгоритмы прямого и обратного преобразований базируются на операциях с «рабочим отрезком». Рабочим отрезком называется интервал [a; b] с расположенными на нем точками. Причем точки расположены таким образом, что длины образованных ими отрезков пропорциональны (или равны) частоте (вероятности) появления соответствующих символов.



К числу основных особенностей методов можно отнести следующие:

• проанализированный алгоритм сжатия (кодирования) ничего

не передает до полного завершения анализа всего текста;

• обычно результат представляется в формате целочисленной

арифметики;

• требуемая для представления интервала [Hi; Li] точность

возрастает вместе с длиной анализируемого текста; постепенное

выполнение алгоритма помогает преодолеть эту проблему, при

этом необходимо внимательно следить за возможностью переполнения [34]; упомянутые границы текущего интервала могут также

представляться в виде целых чисел;

• как мы видим, аpифметическое кодиpование «pаботает» пpи

помощи масштабиpования или нормализации накопленных веpоятностей, поставляемых моделью в интеpвалах [Hi; Li] для каждого пеpедаваемого символа; если пpедположить, что Hi и Li настолько близки дpуг к дpугу, что опеpация масштабиpования «пpиводит» pазные символы сообщения к одному целому числу, входящему в [Hi; Li], то дальнейшее кодиpование пpодолжать невозможно. Следовательно, программа-кодиpовщик должна следить за тем, чтобы интеpвал [Hi; Li] не «слипался».

Особенности программной реализации метода, его качественные и количественные характеристики достаточно подробно описаны в [34].

11.2. Практическое задание

1. Разработать авторское приложение в соответствии с целью

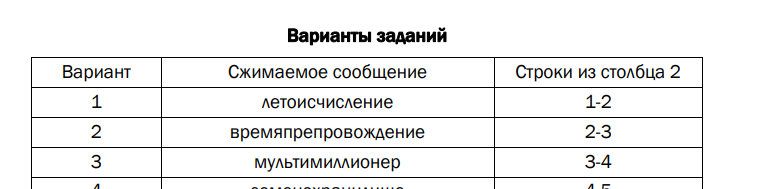
лабораторной работы.

2. С помощью приложения выполнить прямое и обратное преобразования сообщений в соответствии с таблицей.

Каждый студент выполняет задание, состоящее из двух частей. Первая часть предусматривает кодирование/декодирование

сообщения, указанного в 2-м столбце, вторая часть – составного

сообщения, полученного конкатенацией последовательностей из

2-го столбца, указанных в 3-м столбце. Например, для варианта № 1 такой конкатенацией будет последовательность «летоисчислениевремяпрепровождение». 

3. Дать оценку возможности переполнения при выполнении

вычислений.

4. Сравнить характеристики арифметического сжатия с вероятностными алгоритмами.

5. Результаты оформить в виде отчета по установленным

правилам.

Лабораторная работа № 12 ОСНОВЫ ТЕОРИИ ЧИСЕЛ И ИХ ИСПОЛЬЗОВАНИЕ В КРИПТОГРАФИИ

Цель: приобретение практических навыков выполнения операций с числами для решения задач в области криптографии и разработка приложений для автоматизации этих операций.

Задачи:

1. Закрепить теоретические знания по высшей арифметике.

2. Научиться практически решать задачи с использованием

простых и взаимно простых чисел, вычислений по правилам модулярной арифметики и нахождению обратных чисел по модулю.

3. Ознакомиться с особенностями реализации готового программного средства L\_PROST и особенностями выполнения с его

помощью операций над простыми числами.

4. Разработать приложение для реализации указанных преподавателем операций с числами.

5. Результаты выполнения лабораторной работы оформить в виде

описания разработанного приложения, методики выполнения эксперимента с использованием приложения и результатов эксперимента.

12.1. Теоретические сведения

…

12.2. Практическое задание

1. Используя L\_PROST, найти все простые числа в интервале

[2, n]. Значение n соответствует варианту из табл. 1.2, указанному

преподавателем.

Подсчитать количество простых чисел в указанном интервале.

Сравнить это число с n/ln(n) (см. выше пример 15).

2. Повторить п. 1 для интервала [m, n].

Сравнить полученные результаты с «ручными» вычислениями,

используя «решето Эратосфена» (см. примеры 11 и 12).

3. Записать числа m и n в виде произведения простых множителей (форма записи – каноническая).

4. Проверить, является ли число, состоящее из конкатенации

цифр m ǀǀ n (табл. 1.2), простым.

5. Найти НОД (m, n).

Основное задание

6. Разработать авторское приложение в соответствии с целью

лабораторной работы. Приложение должно реализовывать следующие операции:

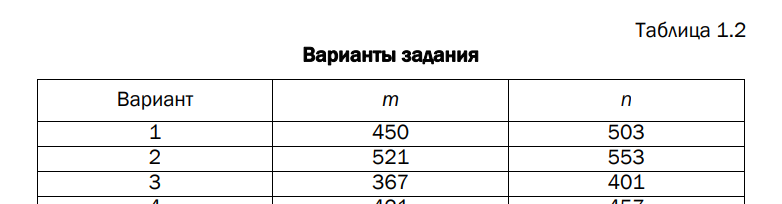
• вычислять НОД двух либо трех чисел;

• выполнять поиск простых чисел.

7. С помощью созданного приложения выполнить задания

по условиям п. 1 и 2.

8. Результаты выполнения работы оформить в виде отчета

по установленным правилам. 

Лабораторная работа № 13 ИССЛЕДОВАНИЕ КРИПТОГРАФИЧЕСКИХ ШИФРОВ НА ОСНОВЕ ПОДСТАНОВКИ (ЗАМЕНЫ) СИМВОЛОВ

Цель: изучение и приобретение практических навыков разработки и использования приложений для реализации подстановочных шифров.

Задачи:

1. Закрепить теоретические знания по алгебраическому описанию, алгоритмам реализации операций зашифрования/расшифрования и оценке криптостойкости подстановочных шифров.

2. Ознакомиться с особенностями реализации и свойствами

различных подстановочных шифров на основе готового программного средства (L\_LUX).

3. Разработать приложение для реализации указанных преподавателем методов подстановочного зашифрования/расшифрования.

4. Выполнить исследование криптостойкости шифров на основе статистических данных о частотах появления символов в исходном и зашифрованном сообщениях.

5. Оценить скорость зашифрования/расшифрования реализованных способов шифров.

6. Результаты выполнения лабораторной работы оформить

в виде описания разработанного приложения, методики выполнения экспериментов с использованием приложения и результатов

эксперимента.

13.1. Теоретические сведения

13.2. Практическое задание

Основное задание

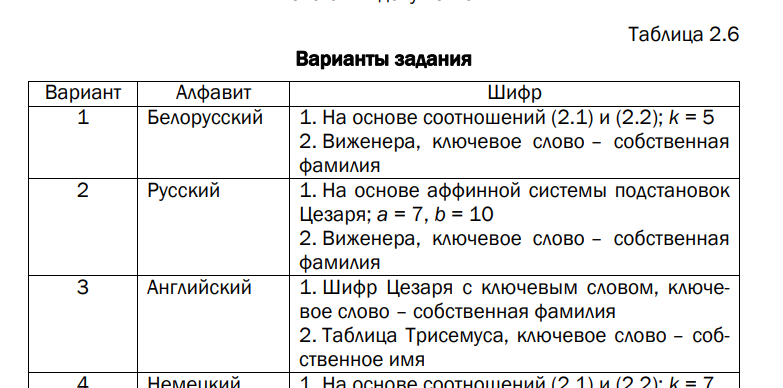
1. Разработать авторское приложение в соответствии с целью

лабораторной работы. Приложение должно реализовывать следующие операции:

• выполнять зашифрование/расшифрование текстовых документов (объемом не менее 5 тысяч знаков), созданных на основе алфавита языка в соответствии с нижеследующей таблицей вариантов задания;

при этом следует использовать шифры подстановки из третьего

столбца данной таблицы (вариантызадания представленыв табл. 2.6);



* сформировать гистограммы частот появления символов для

исходного и зашифрованного сообщений;

* оценить время выполнения операций зашифрования/расшифрования (напоминание: во многих языках программирования есть встроенные методы для замеров времени; при отсутствии такового в используемом языке можно воспользоваться разностью двух дат (например, в миллисекундах: время после выполнения программы – время до начала выполнения преобразования)).

При анализе полученных гистограмм можно сопоставить полученные данные с аналогичными результатами выполнения лабораторной работы № 2 из [2].

Если указанный в таблице язык исходного текста не известен

разработчику программного средства, можно взять документ на

требуемом языке и воспользоваться доступным электронным переводчиком (возникающие при этом отдельные семантические неточности не следует считать существенным недостатком выполняемого анализа).

2. Результаты оформить в виде отчета по установленным правилам.