МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ В.Ф. УТКИНА»

Кафедра «Государственного, муниципального и корпоративного управления»

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

Б1.В.06 Информационная безопасность

Направление подготовки
38.03.04 «Государственное и муниципальное управление»

Направленность (профиль) подготовки – Информационные технологии в государственном и муниципальном управлении

Квалификация выпускника - бакалавр

Формы обучения – очная

Рязань, 2020

1. ОБЩИЕ ПОЛОЖЕНИЯ

Оценочные материалы – это совокупность учебно-методических материалов (контрольных заданий, описаний форм и процедур), предназначенных для оценки качества освоения обучающимися данной дисциплины как части ОПОП ВО.

Цель – оценить соответствие знаний, умений и уровня приобретенных компетенций обучающихся целям и требованиям основной образовательной программы в ходе проведения промежуточной аттестации.

Промежуточная аттестация проводится в форме экзамена. В билет включается 10 тестовых вопросов и три практико-ориентированных задания открытого типа.

2. ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ДИСЦИПЛИНЕ

Контролируемые разделы (темы) дисциплины (результаты по разделам)	Код контролируемой компетенции (или её части)	Наименование оценочного средства
Тема 1. Понятие информационной безопасности. Основные составляющие	ПК-2.1	Зачет
Тема 2. Объектно-ориентированный подход к рассмотрению защищаемых систем. Наиболее распространенные угрозы информационной безопасности и её составляющие	ПК-2.1	Зачет
Тема 3. Законодательный уровень информационной безопасности. Административный уровень информационной безопасности	ПК-2.2	Зачет
Тема 4. Процедурный уровень информационной безопасности	ПК-2.1	Зачет
Тема 5. Основные характеристики программно-технических мер. Идентификация и аутентификация	ПК-2.1	Зачет
Тема 6. Протоколирование и аудит, шифрование, контроль целостности	ПК-2.2	Зачет
Тема 7. Экранирование, анализ защищенности	ПК-2.2	Зачет
Тема 8. Обеспечение высокой доступности	ПК-2.2	Зачет

3. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

На зачете выносится тест, 2 практических контрольных вопроса, 3 задачи и 1 теоретический вопрос. Студент может набрать максимум 35 баллов. Итоговый суммарный балл студента, полученный при прохождении промежуточной аттестации, переводится в традиционную форму по системе «зачтено» / «не зачтено».

Шкала оценивания	Критерий	
зачтено	8 – 20 баллов	Обязательным условием является выполнение всех предусмотренных в течение семестра заданий (на практических работах и при самостоятельной работе)
Не зачтено	0 – 7 баллов	Студент не выполнил всех предусмотренных в течение семестра текущих заданий (на практических работах и при самостоятельной работе)

4. ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

Коды компетенций	*Содержание компетенций*
ПК-2	Способен применять знания основ информационной безопасности, основные положения законодательства о персональных данных, электронной подписи
ПК-2.1	Применяет знания основ информационной безопасности
ПК-2.2	Применяет основные положения законодательства о персональных данных, электронной подписи

а) типовые тестовые вопросы:

ПК-2.1:

1. Информационная безопасность – это:
а) состояние защищенности информационных ресурсов от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства
b) состояние уязвимости информационных ресурсов от внутренних и внешних угроз, способных нанести ущерб интересам личности, общества, государства
c) состояние защищенности граждан от внутренних и внешних угроз, способных нанести ущерб интересам личности

2. Безопасность информации – это:
а) защищенность информации от нежелательного ее разглашения, искажения, утраты или снижения степени доступности информации, а также незаконного ее тиражирования
b) защищенность информации от желательного ее разглашения, искажения, утраты или снижения степени доступности информации, а также незаконного ее тиражирования
c) доступность информации для ее тиражирования

3. Информационная система – это:
а) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств
b) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий
c) совокупность содержащейся в базах данных информации и обеспечивающих ее обработку технических средств

4. _____ – это возможность за приемлемое время получить требуемую информационную услугу (**доступность**)

5. _____ – это защита от несанкционированного доступа к информации (**конфиденциальность**)

6. _____ – это промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется (**окно опасности**)

7. _____ – это потенциальная возможность определенным образом нарушить информационную безопасность (**угроза**)

8. _____ – это попытка реализации угрозы (**атака**)

9. _____ – это код, обладающий способностью к распространению (возможно, с изменениями) путем внедрения в другие программы (**вирусы**)

10. _____ – это код, способный самостоятельно, то есть без внедрения в другие программы, вызывать распространение своих копий по ИС и их выполнение (**черви**)

11. Угроза нарушения конфиденциальности реализуется когда:

а) информация становится известной лицу, не располагающему полномочиями доступа к ней
b) осуществляется несанкционированное изменении информации, хранящейся в информационной системе, или передаваемой из одной системы в другую
c) в результате преднамеренных действий, предпринимаемым другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы

12. Угроза нарушения целостности реализуется когда:
а) осуществляется несанкционированное изменении информации, хранящейся в информационной системе, или передаваемой из одной системы в другую
b) информация становится известной лицу, не располагающему полномочиями доступа к ней
c) в результате преднамеренных действий, предпринимаемым другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы

13. Угроза нарушения доступности реализуется когда:
а) в результате преднамеренных действий, предпринимаемым другим пользователем или злоумышленником, блокируется доступ к некоторому ресурсу вычислительной системы
b) информация становится известной лицу, не располагающему полномочиями доступа к ней
c) осуществляется несанкционированное изменении информации, хранящейся в информационной системе, или передаваемой из одной системы в другую

14. _____ – это выполнение действий под видом лица, обладающего полномочиями для доступа к данным (**маскарад**)

15. Принцип разделения обязанностей предписывает как:
а) распределять роли и ответственность, чтобы один человек не мог нарушить критически важный для организации процесс
b) распределять роли и ответственность, чтобы несколько человек не могли нарушить критически важный для организации процесс
c) распределять роли и ответственность, чтобы один человек мог нарушить критически важный для организации процесс

16. Принцип минимизации привилегий предписывает выделять:
a) пользователям только те права доступа, которые необходимы им для выполнения служебных обязанностей
b) пользователям максимальное количество прав доступа
c) пользователям права доступа, которые необходимы им для выполнения служебных обязанностей, а также некоторые дополнительные права

17. Основной принцип физической защиты формулируется как:
а) "непрерывность защиты в пространстве и времени"
b) "непрерывность защиты в пространстве"
c) "непрерывность защиты во времени"

18. Какие меры позволяют контролировать и при необходимости ограничивать вход и *выход* сотрудников и посетителей? (**меры физического управления доступом**)

19. Реакция на нарушения режима безопасности преследует цели:
a) локализация инцидента и уменьшение наносимого вреда, выявление нарушителя, предупреждение повторных нарушений
b) локализация инцидента и уменьшение наносимого вреда, предупреждение повторных нарушений
b) локализация инцидента и уменьшение наносимого вреда, выявление нарушителя

20. Планирование восстановительных работ позволяет:
а) подготовиться к авариям, уменьшить ущерб от аварий, сохранить способность к функционированию хотя бы в минимальном объеме

b) подготовиться к авариям, сохранить способность к функционированию хотя бы в минимальном объеме
c) уменьшить ущерб от аварий, сохранить способность к функционированию хотя бы в минимальном объеме

21. Корпоративная сеть имеет:
a) несколько территориально разнесенных частей, связи между которыми находятся в ведении внешнего поставщика сетевых услуг, выходя за пределы зоны, контролируемой организацией
b) одну территориально разнесенную часть
c) несколько территориально разнесенных частей, связи между которыми отсутствуют

22. К принципам архитектурной безопасности относятся:
a) непрерывность защиты в пространстве и времени, минимизация привилегий, разделение обязанностей, усиление самого слабого звена
b) непрерывность защиты в пространстве и времени, минимизация привилегий, разделение обязанностей, усиление самого сильного звена
c) непрерывность защиты в пространстве и времени, максимизация привилегий, разделение обязанностей, усиление самого слабого звена

23. Идентификация позволяет субъекту:
a) сообщить своё имя
b) узнать чужое имя
c) изменить своё имя

24. Повысить надежность парольной аутентификации позволяют следующие меры:
a) наложение технических ограничений, управление сроком действия пароля, ограничение доступа к файлу паролей, использование программных генераторов паролей
b) наложение технических ограничений, отсутствие управления сроком действия пароля, ограничение доступа к файлу паролей, использование программных генераторов паролей
c) отсутствие технических ограничений, управление сроком действия пароля, ограничение доступа к файлу паролей, запрет использования программных генераторов паролей

ПК-2.2:

25. Государственная тайна – это:
a) защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации
b) защищаемые организацией сведения в области экономической деятельности, распространение которых может нанести ущерб безопасности организации
c) защищаемые государством сведения в области экономической, деятельности, распространение которых может нанести ущерб безопасности ряда организаций на территории Российской Федерации

26. Служебная тайна содержит:
a) информацию ограниченного распространения, к которой относятся несекретные сведения, касающиеся деятельности организации, ограничения на распространение которых диктуются служебной необходимостью
b) защищаемые государством сведения в области военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации
c) сведения, имеющие действительную или потенциальную коммерческую ценность в силу неизвестности их третьим лицам, когда к ним нет свободного доступа на законном основании и обладатель этих сведений принимает меры к охране их конфиденциальности

27. Какие меры способствуют повышению образованности общества в области информационной безопасности, помогают в разработке и распространении средств обеспечения информационной безопасности? (**направляющие и координирующие меры**)

28. Какие меры направлены на создание и поддержание в обществе негативного отношения к нарушениям и нарушителям информационной безопасности? (**меры ограничительной направленности**)

29. _____ – это лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам (**обладатель информации**)

30. _____ – это возможность получения информации и ее использования (**доступ к информации**)

31. _____ – это обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя (**конфиденциальность информации**)

32. _____ – это действия, направленные на получение информации определенным кругом лиц или передачу информации определенному кругу лиц (**предоставление информации**)

33. _____ – это действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц (**распространение информации**)

34. _____ – это любое действие или совокупность действий, совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение, извлечение, использование, передачу, обезличивание, блокирование, удаление, уничтожение персональных данных (**обработка персональных данных**)

35. _____ – это обработка персональных данных с помощью средств вычислительной техники (**автоматизированная обработка персональных данных**)

36. _____ – это действия, направленные на раскрытие персональных данных неопределенному кругу лиц (**распространение персональных данных**)

37. _____ – это действия, направленные на раскрытие персональных данных определенному лицу или определенному кругу лиц (**предоставление персональных данных**)

38. _____ – это временное прекращение обработки персональных данных (**блокирование персональных данных**)

39. _____ – это действия, в результате которых становится невозможным восстановить содержание персональных данных в информационной системе персональных данных и (или) в результате которых уничтожаются материальные носители персональных данных (**уничтожение персональных данных**)

40. Для обеспечения высокой доступности необходимо соблюдать следующие принципы архитектурной безопасности:
a) внесение в конфигурацию избыточности, наличие средств обнаружения внештатных ситуаций, наличие средств реконфигурирования для восстановления, отсутствие единой точки отказа
b) внесение в конфигурацию избыточности, наличие средств обнаружения внештатных ситуаций, наличие средств реконфигурирования для восстановления, наличие единой точки отказа

c) внесение в конфигурацию избыточности, отсутствие средств обнаружения внештатных ситуаций, наличие средств реконфигурирования для восстановления, отсутствие единой точки отказа

41. Под протоколированием понимается:
a) сбор и накопление информации о событиях, происходящих в информационной системе
b) сбор и накопление информации об операциях аутентификации, происходящих в информационной системе
c) сбор и накопление информации об операциях с файлами, происходящих в информационной системе

42. Аудит – это:
a) анализ накопленной информации, проводимый оперативно, в реальном времени или периодически
b) анализ накопленной информации, проводимый нерегулярно
c) накопление информации во времени

43. Сигнатура атаки – это:
a) совокупность условий, при выполнении которых атака считается имеющей место, что вызывает заранее определенную реакцию
b) совокупность условий, при выполнении которых атака считается несостоявшейся
c) совокупность условий, при выполнении которых атака считается имеющей место, что не вызывает заранее определенной реакции

44. В симметричном шифровании используется:
a) один ключ
b) два ключа
c) три ключа

45. Хэш-функция – это:
a) труднообратимое преобразование данных, реализуемое средствами симметричного шифрования со связыванием блоков
b) легкообратимое преобразование данных, реализуемое средствами симметричного шифрования со связыванием блоков
c) средство архивирования данных

46. Экран – это:
a) средство разграничения доступа клиентов из одного множества к серверам из другого множества
b) средство доступа клиентов из одного множества к серверам из другого множества
c) средство доступа клиентов между рабочими станциями сети

47. Отказ – это:
a) событие, которое заключается в нарушении работоспособности изделия
b) событие, которое заключается в нарушении доступа к изделию
c) событие, которое заключается в улучшении работоспособности изделия

б) практико-ориентированные задания открытого типа:

ПК-2.1:

1. Пароль состоит из 5 букв русского алфавита. При этом в системе хранится не сам пароль, а его ключ, который формируется по следующему принципу. Каждой букве алфавита ставится в соответствие определенное число (А – 1, Б – 2, В – 3 и т.д.). Когда пользователь выбирает себе пароль, КЕПКА, то буквам пароля ставятся в соответствие следующие числа – К – 12, Е – 6, П –

17, К – 12, А – 1, а затем вычисляется следующая сумма – 12 + 6 + 17 + 12 + 1 = 48. Это число и есть ключ. Будет ли такая система формирования ключа надежной?
Ответ: Система **не будет** надежной. Например, если для указанного в задаче случая взять слово КККЕЕ, то для него сумма будет равна также 48 (12 + 12 + 12 + 6 + 6). То есть можно подобрать такое сочетание букв, что рассчитанная в результате сумма будет совпадать с искомой. Можно подобрать различные пары паролей, образующие коллизии, например, АБВГД и БББГД, АЕЗНТ и БДИЛУ.

2. Перед группой хакеров стоит задача по выводу из строя компьютеров конкурирующей фирмы. Они создали вредоносное программное обеспечение, распространяющееся в сети. В силу особенностей разработки вирус при распространении с зараженного компьютера всегда поражает либо 4, либо 6 ещё не зараженных. В случае если такого количества незараженных компьютеров нет, то он не имеет возможности распространяться. В сети фирмы зарегистрировано 257 компьютеров. Возможно ли заражение всех компьютеров фирмы при условии, что изначально заражается один компьютер. Если возможно, то приведите пример цепочки заражения.
Ответ: Заражение возможно, если хотя бы одна из цепочек заражения может привести к полному заражению сети. Рассмотрим возможные цепочки заражения. Изначально заражен 1 компьютер и не заражено 256.
1 этап заражения. Зараженный компьютер распространяет вирус либо на 4 компьютера, либо на 6 компьютеров. В результате возможно две ситуации: 5 зараженных и 252 не зараженных компьютера и 7 зараженных и 250 не зараженных компьютеров.
2 этап. Возьмем первую ситуацию. Так как незараженных компьютеров еще достаточно, каждый из зараженных будет распространять вирус. Возможны следующие ситуации:
– каждый из 5 компьютеров распространил вирус на 6 незараженных. Итого 35 компьютеров заражено, 222 остаются незараженными.
– один компьютер отправил вирус на 4 незараженных, каждый из остальных 4 компьютеров распространил вирус на 6 незараженных. Итого 33 компьютера заражено, 224 остаются незараженными.
…
– каждый из 5 компьютеров распространил вирус на 4 незараженных. Итого 25 компьютеров заражено, 232 остаются незараженными.
3 этап. Опять же для примера возьмем 1 ситуацию исхода предыдущего этапа. Возможные исходы: все 35 компьютеров заражают по 6 (итого 245 зараженных, 12 незараженных), 34 по 6 и 1 по 4 (итого 243 зараженных и 14 незараженных) и так далее. И снова обратимся к 1 ситуации, осталось 12 незараженных.
Проверим, возможно ли их заражение на последнем этапе. Заразить 12 компьютеров могут вместе 3 зараженных, распространив вирус на 4 компьютера каждый, либо 2 заражённых, распространив вирус на 6. Это и будет пример цепочки заражения.
Таким образом, **заражение возможно**.

3. Выполнить шифрование с помощью шифра Атбаш фразы «начинайте подготовку к экзамену». Количество символов в алфавите n = 34.
Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц

К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

н -> т:
а -> ‘ ‘
ч -> и
…
В итоге получаем текст:
т ичт цныарсьэнсюхмахагхш уытм

4. Выполнить шифрование с помощью шифра Атбаш фразы «завтра зачет». Количество символов в алфавите n = 34.
Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н

У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

з -> ш
а -> ‘ ‘
в -> ю
т -> н
р -> п
а -> ‘ ‘
‘ ‘ -> а
з -> ш
а -> ‘ ‘
ч -> и
е -> ы
т -> н

В итоге получаем текст:
ш юнп аш иын

5. Выполнить шифрование с помощью шифра Атбаш фразы «скоро сессия». Количество символов в алфавите n = 34.
Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л

Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:

охспсаоыоочб

6. Выполнить шифрование с помощью шифра Атбаш фразы «сегодня концерт». Количество символов в алфавите n = 34.

Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:

оыэсьтбахстйыпн

7. Выполнить шифрование с помощью шифра Атбаш фразы «зайди в деканат». Количество символов в алфавите n = 34.

Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:

ш цьчаюаьых т н

8. Выполнить шифрование с помощью шифра Атбаш фразы «собери урожай». Количество символов в алфавите n = 34.

Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы

Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:
осяыпчампсщ ц

9. Выполнить шифрование с помощью шифра Атбаш фразы «помой пол». Количество символов в алфавите n = 34.
Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О

Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:
рсусцарсф

10. Выполнить шифрование с помощью шифра Атбаш фразы «реши задачу». Количество символов в алфавите n = 34.

Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В

Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:
пызчаш ь им

11. Выполнить шифрование с помощью шифра Атбаш фразы «приготовь обед». Количество символов в алфавите n = 34.
Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:
рпчэснсюдасяыь

12. Выполнить шифрование с помощью шифра Атбаш фразы «испеки пирог». Количество символов в алфавите n = 34.
Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я

В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:
чорыхчарчпсэ

13. Выполнить шифрование с помощью шифра Атбаш фразы «заштопай брюки». Количество символов в алфавите n = 34.
Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т

О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:
ш знср цаяпвхч

14. Выполнить шифрование с помощью шифра Атбаш фразы «зайди во двор». Количество символов в алфавите n = 34.
Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё

Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:
ш цьчаюсаьюсп

15. Выполнить шифрование с помощью шифра Атбаш фразы «выходи из леса». Количество символов в алфавите n = 34.
Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:
юексьчачшафыо

16. Выполнить шифрование с помощью шифра Атбаш фразы «готовь отчет». Количество символов в алфавите n = 34.
Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:
эснсюдасниын

17. Выполнить шифрование с помощью шифра Атбаш фразы «скоро зима». Количество символов в алфавите n = 34.
Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х

Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:
охспсашчу

18. Выполнить шифрование с помощью шифра Атбаш фразы «убери мусор». Количество символов в алфавите n = 34.

Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И

Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:
мяыпчаумосп

19. Выполнить шифрование с помощью шифра Атбаш фразы «напои собаку». Количество символов в алфавите n = 34.
Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:
т рсчаося хм

20. Выполнить шифрование с помощью шифра Атбаш фразы «покорми кота». Количество символов в алфавите n = 34.

Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:

рсхспучахсн

21. Выполнить шифрование с помощью шифра Атбаш фразы «готовься к лабораторной». Количество символов в алфавите n = 34.

Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ

Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:
эснсюдобахаф ясп нсптсц

22. Выполнить шифрование с помощью шифра Атбаш фразы «выйди в коридор». Количество символов в алфавите n = 34.
Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н

У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:

юецьчаюахспчьсп

23. Выполнить шифрование с помощью шифра Атбаш фразы «купи хлеб». Количество символов в алфавите n = 34.

Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б

‘ ‘(пробел)	А

В итоге получаем текст:
хмрчакфыя

24. Выполнить шифрование с помощью шифра Атбаш фразы «обед готов». Количество символов в алфавите n = 34.
Ответ: Алгоритм шифрования заключается в замене k-го символа алфавита символом с порядковым номером n - k + 1, где n – количество символов в алфавите.

Символ исходный	Символ закодированный
А	‘ ‘(пробел)
Б	Я
В	Ю
Г	Э
Д	Ь
Е	Ы
Ё	Ъ
Ж	Щ
З	Ш
И	Ч
Й	Ц
К	Х
Л	Ф
М	У
Н	Т
О	С
П	Р
Р	П
С	О
Т	Н
У	М
Ф	Л
Х	К
Ц	Й
Ч	И
Ш	З
Щ	Ж
Ъ	Ё
Ы	Е
Ь	Д
Э	Г
Ю	В
Я	Б
‘ ‘(пробел)	А

В итоге получаем текст:
сяыьаэснсю

25. Для входа в систему используется пароль, состоящий из трёх двузначных чисел, расположенных следующим образом: xx-xx-xx Известно, что пароль состоит из 3-х неповторяющихся простых чисел. При этом, последняя цифра первого числа равна первой цифре второго числа, а последняя цифра второго числа равна первой цифре третьего числа. Пример: x1-17-7y Задержка между попытками входа в систему равна 1 секунде. За какое минимальное время (в секундах) можно гарантированно получить пароль, если на ввод пароля время не тратится, и количество попыток ввода пароля не ограничено?
Ответ: Для начала необходимо найти все простые числа в диапазоне от 11 до 99 (двузначные числа). Простым является такое число, которое делится только на себя и на 1. Сделать это можно

перебором, проверяя, не делится ли проверяемое число на какое-либо от 2-х до самого числа (либо половины числа).
Для ускорения напишем программу, которая выводит на экран все простые числа в указанном диапазоне.
Листинг программы на языке С.

```
// Функция, определяющая, является ли число простым
// ПАРАМЕТР:
// n - проверяемое число
// ВОЗВРАЩАЕТ:
// true - число n простое
// false - число n непростое
bool isprime(int n)
 {
   if (n == 1)
     return true;
   for (int d = 2; d < n / 2; d++)
     if (n % d == 0)
       return false;
  return true;
}
int main()
 {
   // Цикл перебора чисел от 11 до 99
   // Для каждого числа вызывается функция isprime()
   // Если функция вернула true - число добавляется в массив
   // Счетчик Count считает количество простых чисел
   int Count = 0;
   int list_input[100] = { 0 };
   // Формирование массива простых чисел
   for (int x = 11; x < 100; x++)
    {
      if (isprime(x) == true)
       {
         list_input[Count] = x;
         Count += 1;
        }
    }
   // Вывод на экран
   for (int i = 0; i < Count; i++)
    {
      printf("%d ", list_input[i]);
     }
    printf("\nTotal: %d\n", Count);
   return 0;
 }
```

Результат работы программы:
11 13 17 19 23 29 31 37 41 43 47 53 59 61 67 71 73 79 83 89 97
Total: 21
Всего 21 простых чисел в диапазоне от 11 до 99. Теперь необходимо выделить все возможные комбинации, удовлетворяющие условию «последняя цифра первого числа равна первой цифре второго числа, а последняя цифра второго числа равна первой цифре третьего числа».
Сделать это можно перебором всех комбинаций. В цикле перебираем всевозможные числа и проверяем два условия:
– все числа разные;
– последняя цифра первого числа равна первой цифре второго числа, а последняя цифра второго числа равна первой цифре третьего числа.

Если все условия выполнены, то увеличиваем значение счетчика. В результате счетчик будет содержать количество комбинаций, удовлетворяющих заданию. Поскольку задержка между вводом паролей равна 1 секунде, а после ввода последней комбинации задержки нет, то ответ – количество найденных комбинаций минус 1.

Листинг программы:

```
// Функция выводит на экран все комбинации,
// удовлетворяющие условию
// ПАРАМЕТРЫ:
// list_input - массив чисел, из которых будут строится комбинации
// count - количество чисел в массиве list_input
// ВОЗВРАЩАЕТ:
// выводит на экран комбинации, удовлетворяющие условию
// выводит на экран количество комбинаций
void combination(int list_input[], int count)
 {
   int last_digit1;
   int first_digit2;
   int last_digit2;
   int first_digit3;
   int total = 0;
   for (int i = 0; i < count; i++)
     for (int j = 0; j < count; j++)
       for (int k = 0; k < count; k++)
        {
          if ( list_input[i] != list_input[j] && list_input[j] != list_input[k] && list_input[i] != list_input[k] )
            {
              // последняя цифра числа
              last_digit1 = list_input[i] % 10;
              // первая цифра числа
              first_digit2 = list_input[j] / 10;
              last_digit2 = list_input[j] % 10;
              first_digit3 = list_input[k] / 10;
              if ( last_digit1 == first_digit2 && last_digit2 == first_digit3 )
               {
                 printf("%d-%d-%d\n", list_input[i], list_input[j], list_input[k]);
                 total++;
               }
            }
        }
   // Вывод общего количества комбинаций
   printf("Total: %d\n", total);
 }
```

В результате выполнения программы получим следующие данные: 11-13-31, 11-13-37, 11-17-71, 11-17-73, 11-17-79, 11-19-97, 13-31-11, 13-31-17, 13-31-19, 13-37-71, 13-37-73, 13-37-79, 17-71-11, 17-71-13, 17-71-19, 17-73-31, 17-73-37, 17-79-97, 19-97-71, 19-97-73, 19-97-79, 23-31-11, 23-31-13, 23-31-17, 23-31-19, 23-37-71, 23-37-73, 23-37-79, 29-97-71, 29-97-73, 29-97-79, 31-11-13, 31-11-17, 31-11-19, 31-13-37, 31-17-71, 31-17-73, 31-17-79, 31-19-97, 37-71-11, 37-71-13, 37-71-17, 37-71-19, 37-73-31, 37-79-97, 41-11-13, 41-11-17, 41-11-19, 41-13-31, 41-13-37, 41-17-71, 41-17-73, 41-17-79, 41-19-97, 43-31-11, 43-31-13, 43-31-17, 43-31-19, 43-37-71, 43-37-73, 43-37-79, 47-71-11, 47-71-13, 47-71-17, 47-71-19, 47-73-31, 47-73-37, 47-79-97, 53-31-11, 53-31-13, 53-31-17, 53-31-19, 53-37-71, 53-37-73, 53-37-79, 59-97-71, 59-97-73, 59-97-79, 61-11-13, 61-11-17, 61-11-19, 61-13-31, 61-13-37, 61-17-71, 61-17-73, 61-17-79, 61-19-97, 67-71-11, 67-71-13, 67-71-17, 67-71-19, 67-73-31, 67-73-37, 67-79-97, 71-11-13, 71-11-17, 71-11-19, 71-13-31, 71-13-37, 71-17-73, 71-17-79, 71-19-97, 73-31-11, 73-31-13, 73-31-17, 73-31-19, 73-37-71, 73-37-79, 79-97-71, 79-97-73, 83-31-11, 83-31-13, 83-31-17, 83-31-19, 83-37-71, 83-37-73, 83-37-79, 89-97-71, 89-97-73, 89-97-79, 97-71-11, 97-71-13, 97-71-17, 97-71-19, 97-73-31, 97-73-37 Total: 126

Всего таких комбинаций будет 126, следовательно, максимальное затраченное время будет равно (126 – 1) * 1 сек = 125 сек.
Таким образом, минимальное время, за которое можно гарантированно получить пароль, равно **125** секунд.

ПК-2.2:

26. Выполнить шифрование с помощью шифра Цезаря для ключа = 1 фразы «начинайте подготовку к экзамену».
Ответ: воспользуемся алфавитом из таблицы.

Символ	Номер
А	0
Б	1
В	2
Г	3
Д	4
Е	5
Ё	6
Ж	7
З	8
И	9
Й	10
К	11
Л	12
М	13
Н	14
О	15
П	16
Р	17
С	18
Т	19
У	20
Ф	21
Х	22
Ц	23
Ч	24
Ш	25
Щ	26
Ъ	27
Ы	28
Ь	29
Э	30
Ю	31
Я	32

Математически шифр Цезаря можно описать следующими формулами:

$$\text{Encrypt}(m_n) = (Q + m_n + k) \% Q, \quad (1)$$

$$\text{Decrypt}(c_n) = (Q + c_n - k) \% Q. \quad (2)$$

где m – открытый текст;
k – ключ шифрования;
Q – количество символов в алфавите;
c – зашифрованный текст;
оператор % вычисляет остаток после деления первого операнда на второй.
1) символ “н”:
Encrypt = (33 + 14 + 1) % 33 = 48 % 33 = 15. Получили н -> о

2) символ “а”:
Encrypt = (33 + 0 + 1) % 33 = 34 % 33 = 1. Получили а -> б
3) символ “ч”:
Encrypt = (33 + 24 + 1) % 33 = 58 % 33 = 25. Получили ч -> ш
…

В итоге получаем текст:
обшйобкуё рпедпупглф л юлибнёоф

27. Выполнить шифрование с помощью шифра Цезаря для ключа = 2 фразы «решайте задачу».
Ответ: воспользуемся алфавитом из таблицы.

Символ	Номер
А	0
Б	1
В	2
Г	3
Д	4
Е	5
Ё	6
Ж	7
З	8
И	9
Й	10
К	11
Л	12
М	13
Н	14
О	15
П	16
Р	17
С	18
Т	19
У	20
Ф	21
Х	22
Ц	23
Ч	24
Ш	25
Щ	26
Ъ	27
Ы	28
Ь	29
Э	30
Ю	31
Я	32

Математически шифр Цезаря можно описать следующими формулами:

$$\text{Encrypt}(m_n) = (Q + m_n + k) \% Q, \quad (1)$$

$$\text{Decrypt}(c_n) = (Q + c_n - k) \% Q. \quad (2)$$

где m – открытый текст;
k – ключ шифрования;
Q – количество символов в алфавите;
c – зашифрованный текст;
оператор % вычисляет остаток после деления первого операнда на второй.

В итоге получаем текст:
тжъвлфж йвёвщх

28. Выполнить шифрование с помощью шифра Цезаря для ключа = 3 фразы «тяните билет».
Ответ: воспользуемся алфавитом из таблицы.

Символ	Номер
А	0
Б	1
В	2
Г	3
Д	4
Е	5
Ё	6
Ж	7
З	8
И	9
Й	10
К	11
Л	12
М	13
Н	14
О	15
П	16
Р	17
С	18
Т	19
У	20
Ф	21
Х	22
Ц	23
Ч	24
Ш	25
Щ	26
Ъ	27
Ы	28
Ь	29
Э	30
Ю	31
Я	32

Математически шифр Цезаря можно описать следующими формулами:

$$\text{Encrypt}(m_n) = (Q + m_n + k) \% Q, \quad (1)$$

$$\text{Decrypt}(c_n) = (Q + c_n - k) \% Q. \quad (2)$$

где m – открытый текст;
k – ключ шифрования;
Q – количество символов в алфавите;
c – зашифрованный текст;
оператор % вычисляет остаток после деления первого операнда на второй.

В итоге получаем текст:

хврлхз длозх

29. Выполнить шифрование с помощью шифра Цезаря для ключа = 4 фразы «приближается сессия».
Ответ: воспользуемся алфавитом из таблицы.

Символ	Номер
А	0
Б	1
В	2
Г	3

Д	4
Е	5
Ё	6
Ж	7
З	8
И	9
Й	10
К	11
Л	12
М	13
Н	14
О	15
П	16
Р	17
С	18
Т	19
У	20
Ф	21
Х	22
Ц	23
Ч	24
Ш	25
Щ	26
Ъ	27
Ы	28
Ь	29
Э	30
Ю	31
Я	32

Математически шифр Цезаря можно описать следующими формулами:

$$\text{Encrypt}(m_n) = (Q + m_n + k) \% Q, \quad (1)$$

$$\text{Decrypt}(c_n) = (Q + c_n - k) \% Q. \quad (2)$$

где m – открытый текст;
k – ключ шифрования;
Q – количество символов в алфавите;
c – зашифрованный текст;
оператор % вычисляет остаток после деления первого операнда на второй.

В итоге получаем текст:

уфмепмкдицхг хиххмг

30. Выполнить шифрование с помощью шифра Цезаря для ключа = 5 фразы «собирайтесь на лекцию».

Ответ: воспользуемся алфавитом из таблицы.

Символ	Номер
А	0
Б	1
В	2
Г	3
Д	4
Е	5
Ё	6
Ж	7
З	8
И	9
Й	10

К	11
Л	12
М	13
Н	14
О	15
П	16
Р	17
С	18
Т	19
У	20
Ф	21
Х	22
Ц	23
Ч	24
Ш	25
Щ	26
Ъ	27
Ы	28
Ь	29
Э	30
Ю	31
Я	32

Математически шифр Цезаря можно описать следующими формулами:

$$\text{Encrypt}(m_n) = (Q + m_n + k) \% Q, \quad (1)$$

$$\text{Decrypt}(c_n) = (Q + c_n - k) \% Q. \quad (2)$$

где m – открытый текст;
k – ключ шифрования;
Q – количество символов в алфавите;
c – зашифрованный текст;
оператор % вычисляет остаток после деления первого операнда на второй.

В итоге получаем текст:

цуёнхеочйцб те рйпынг

31. Выполнить шифрование с помощью шифра Цезаря для ключа = 6 фразы «купи колбасу».

Ответ: воспользуемся алфавитом из таблицы.

Символ	Номер
А	0
Б	1
В	2
Г	3
Д	4
Е	5
Ё	6
Ж	7
З	8
И	9
Й	10
К	11
Л	12
М	13
Н	14
О	15
П	16
Р	17
С	18

Т	19
У	20
Ф	21
Х	22
Ц	23
Ч	24
Ш	25
Щ	26
Ъ	27
Ы	28
Ь	29
Э	30
Ю	31
Я	32

Математически шифр Цезаря можно описать следующими формулами:

$$\text{Encrypt}(m_n) = (Q + m_n + k) \% Q, \quad (1)$$

$$\text{Decrypt}(c_n) = (Q + c_n - k) \% Q. \quad (2)$$

где m – открытый текст;
k – ключ шифрования;
Q – количество символов в алфавите;
c – зашифрованный текст;
оператор % вычисляет остаток после деления первого операнда на второй.

В итоге получаем текст:

рщхо рфсжёчщ

32. Выполнить шифрование с помощью шифра Цезаря для ключа = 7 фразы «покорми рыбок».
Ответ: воспользуемся алфавитом из таблицы.

Символ	Номер
А	0
Б	1
В	2
Г	3
Д	4
Е	5
Ё	6
Ж	7
З	8
И	9
Й	10
К	11
Л	12
М	13
Н	14
О	15
П	16
Р	17
С	18
Т	19
У	20
Ф	21
Х	22
Ц	23
Ч	24
Ш	25
Щ	26

Ъ	27
Ы	28
Ь	29
Э	30
Ю	31
Я	32

Математически шифр Цезаря можно описать следующими формулами:

$$\text{Encrypt}(m_n) = (Q + m_n + k) \% Q, \quad (1)$$

$$\text{Decrypt}(c_n) = (Q + c_n - k) \% Q. \quad (2)$$

где m – открытый текст;
k – ключ шифрования;
Q – количество символов в алфавите;
c – зашифрованный текст;
оператор % вычисляет остаток после деления первого операнда на второй.

В итоге получаем текст:

цхсхчуп чвзхс

33. Выполнить шифрование с помощью шифра Цезаря для ключа = 8 фразы «свари суп».

Ответ: воспользуемся алфавитом из таблицы.

Символ	Номер
А	0
Б	1
В	2
Г	3
Д	4
Е	5
Ё	6
Ж	7
З	8
И	9
Й	10
К	11
Л	12
М	13
Н	14
О	15
П	16
Р	17
С	18
Т	19
У	20
Ф	21
Х	22
Ц	23
Ч	24
Ш	25
Щ	26
Ъ	27
Ы	28
Ь	29
Э	30
Ю	31
Я	32

Математически шифр Цезаря можно описать следующими формулами:

$$\text{Encrypt}(m_n) = (Q + m_n + k) \% Q, \quad (1)$$
$$\text{Decrypt}(c_n) = (Q + c_n - k) \% Q. \quad (2)$$

где m – открытый текст;
k – ключ шифрования;
Q – количество символов в алфавите;
c – зашифрованный текст;
оператор % вычисляет остаток после деления первого операнда на второй.

В итоге получаем текст:

щйзшр щыч

34. Выполнить шифрование с помощью шифра Цезаря для ключа = 9 фразы «приготовь завтрак».

Ответ: воспользуемся алфавитом из таблицы.

Символ	Номер
А	0
Б	1
В	2
Г	3
Д	4
Е	5
Ё	6
Ж	7
З	8
И	9
Й	10
К	11
Л	12
М	13
Н	14
О	15
П	16
Р	17
С	18
Т	19
У	20
Ф	21
Х	22
Ц	23
Ч	24
Ш	25
Щ	26
Ъ	27
Ы	28
Ь	29
Э	30
Ю	31
Я	32

Математически шифр Цезаря можно описать следующими формулами:

$$\text{Encrypt}(m_n) = (Q + m_n + k) \% Q, \quad (1)$$
$$\text{Decrypt}(c_n) = (Q + c_n - k) \% Q. \quad (2)$$

где m – открытый текст;
k – ключ шифрования;
Q – количество символов в алфавите;
c – зашифрованный текст;
оператор % вычисляет остаток после деления первого операнда на второй.

В итоге получаем текст:

шщслчычке рикыщиу

35. Выполнить шифрование с помощью шифра Цезаря для ключа = 10 фразы «заведи кота».
Ответ: воспользуемся алфавитом из таблицы.

Символ	Номер
А	0
Б	1
В	2
Г	3
Д	4
Е	5
Ё	6
Ж	7
З	8
И	9
Й	10
К	11
Л	12
М	13
Н	14
О	15
П	16
Р	17
С	18
Т	19
У	20
Ф	21
Х	22
Ц	23
Ч	24
Ш	25
Щ	26
Ъ	27
Ы	28
Ь	29
Э	30
Ю	31
Я	32

Математически шифр Цезаря можно описать следующими формулами:

$$\text{Encrypt}(m_n) = (Q + m_n + k) \% Q, \quad (1)$$

$$\text{Decrypt}(c_n) = (Q + c_n - k) \% Q. \quad (2)$$

где m – открытый текст;
k – ключ шифрования;
Q – количество символов в алфавите;
c – зашифрованный текст;
оператор % вычисляет остаток после деления первого операнда на второй.

В итоге получаем текст:
сйлонт фшьй

36. Выполнить шифрование с помощью шифра Цезаря для ключа = 11 фразы «завтра выходной».
Ответ: воспользуемся алфавитом из таблицы.

Символ	Номер
А	0
Б	1
В	2

Г	3
Д	4
Е	5
Ё	6
Ж	7
З	8
И	9
Й	10
К	11
Л	12
М	13
Н	14
О	15
П	16
Р	17
С	18
Т	19
У	20
Ф	21
Х	22
Ц	23
Ч	24
Ш	25
Щ	26
Ъ	27
Ы	28
Ь	29
Э	30
Ю	31
Я	32

Математически шифр Цезаря можно описать следующими формулами:

$$\text{Encrypt}(m_n) = (Q + m_n + k) \% Q, \quad (1)$$

$$\text{Decrypt}(c_n) = (Q + c_n - k) \% Q. \quad (2)$$

где m – открытый текст;
k – ключ шифрования;
Q – количество символов в алфавите;
c – зашифрованный текст;
оператор % вычисляет остаток после деления первого операнда на второй.

В итоге получаем текст:

ткмэык мёащошщф

37. Выполнить шифрование с помощью шифра «Квадрат Полибия» фразы «начинайте подготовку к экзамену», используя ключ «зачет».

Ответ: составим исходную таблицу для русского языка без учета ключа.

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	‘ ‘	1	2

Построим таблицу с учетом ключа «зачет» (без повторения символов).

	1	2	3	4	5	6
1	**З**	**А**	**Ч**	**Е**	**Т**	Б
2	В	Г	Д	Ё	Ж	И

3	Й	К	Л	М	Н	О
4	П	Р	С	У	Ф	Х
5	Ц	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	‘ ‘	1	2

Осуществим кодирование:
н -> л
а -> з
ч -> ц
и -> ё
н -> л
а -> з
й -> ж
т -> р
е -> б
 ->
п -> н
о -> м
д -> т
г -> е
о -> м
т -> р
о -> м
в -> ч
к -> и
у -> с
 ->
к -> и
 ->
э -> э
к -> и
з -> д
а -> з
м -> к
е -> б
н -> л
у -> с
Получим зашифрованное сообщение:
лзцёлзжрб нмтемрмчис и эидзкблс

38. Выполнить шифрование с помощью шифра Скитала фразы «скоро зима», используя диаметр цилиндра = 3.
Ответ: сомк аоз ри

39. Выполнить шифрование с помощью шифра Скитала фразы «завтра зачет», используя диаметр цилиндра = 4.
Ответ: зт чарзеваат

40. Выполнить шифрование с помощью шифра Скитала фразы «почисти картошку», используя диаметр цилиндра = 5.
Ответ: пско оташ чирк и ту

41. Выполнить шифрование с помощью шифра Скитала фразы «годовой отчет», используя диаметр цилиндра = 6.
Ответ: гойтт ов ч доое

42. Выполнить шифрование с помощью шифра Скитала фразы «весна опять пришла», используя диаметр цилиндра = 7.

Ответ: внотпш еапьрл с я иа

43. Выполнить шифрование с помощью шифра Скитала фразы «готов к труду», используя диаметр цилиндра = 4.
Ответ: гвтуо р тку о д

44. Выполнить шифрование с помощью шифра Скитала фразы «много работы», используя диаметр цилиндра = 5.
Ответ: мгро ноат о бы

45. Выполнить шифрование с помощью шифра Скитала фразы «тебя вызвали в деканат», используя диаметр цилиндра = 6.
Ответ: т в еаевавктбыл а язидн

46. Выполнить шифрование с помощью шифра Скитала фразы «окончание учебного года», используя диаметр цилиндра = 7.
Ответ: очеего ка бод онун а ничог

47. Первокурсник Иван был крайне взволнован, когда его одногруппница Анна выложила в соцсети подборку песен и картинок с загадочной подписью: 29 лкдкюеюжейк Зная, что Анна увлекается криптографией, помогите Ивану выяснить, что же написала девушка.
Ответ: Из условий задачи понятно, что подпись зашифрована шифром Цезаря с ключом 29. Для расшифровки используем нумерованный алфавит из приложения. При расшифровке номер буквы в шифр-тексте сдвигается влево на размер ключа. Составим таблицу дешифровки

Шифр-текст	л	к	д	к	ю	е	ю	ж	е	й	к
Номер буквы в шифр-тексте	13	12	5	12	32	6	32	8	6	11	12
Ключ	29	29	29	29	29	29	29	29	29	29	29
Номер буквы исходного текста	17	16	9	16	3	10	3	12	10	15	16
Исходный текст	п	о	з	о	в	и	в	к	и	н	о

Получили расшифрованное сообщение: позови в кино

48. Дети играли в прятки, и мальчик И. оказался закрытым в подвале. Он не мог открыть дверь изнутри, и стал внимательно осматривать помещение. Внезапно И. увидел клочок бумаги, который завалился под старый запыленный шкаф. Мальчик прочитал написанное: впоыиюяехтыбчвпжнпфж На обратной стороне бумаги все буквы размыло, но можно было разобрать слова: «квадрат… шесть на пять … и/й …. е/ё… ь/ъ». Возможно ли, что спасение сокрыто в этом послании? Помогите И. разгадать загадку.
Ответ: По словам на обратной стороне бумаги можно понять, что речь идет о шифре «квадрат Полибия» с пояснением, что таблица шифрования состоит из 6 столбцов и 5 строк (также есть другие вариации шифра, с квадратом 6 на 6 и 5 на 5). Так как русский алфавит 33 символа (он не влезет в таблицу 6 на 5), в тексте дано пояснение, какие буквы необходимо объединить в одну ячейку матрицы шифрования. Составим матрицу шифрования

	1	2	3	4	5	6
1	а	б	в	г	д	е/ё
2	ж	з	и/й	к	л	м
3	н	о	п	р	с	т
4	у	ф	х	ц	ч	ш
5	щ	ы	ь/ъ	э	ю	я

Составим таблицу координат зашифрованного текста. Первая строка – зашифрованный текст по буквам. Вторая и третья строки – номер столбца и номер строки буквы в матрице шифрования соответственно. Запишем в таблицу координаты букв зашифрованного текста.

	в	п	о	ы	и	ю	я	е	х	т	ы	б	ч	в	п	ж	н	п	ф	ж
столбец	3	3	2	2	3	5	6	6	3	6	2	2	5	3	3	1	1	3	2	1
строка	1	3	3	5	2	5	5	1	4	3	5	1	4	1	3	2	3	3	4	2

Выпишем координаты букв в виде столбец-строка по порядку в две строки. Например, для первых двух букв координаты будут выглядеть следующим образом: 31 33. Количество цифр в каждой строке должно быть равно количеству букв в зашифрованной фразе.
31 33 23 25 32 55 65 61 34 63
25 21 54 31 33 12 13 33 24 12
Первая строка – первая координата буквы в исходной фразе – номер столбца. Вторая строка – вторая координата буквы в исходной фразе – номер строки.
Составим матрицу координат исходного текста и найдём новые значения в «квадрате Полибия»:

столбец	3	1	3	3	2	3	2	5	3	2	5	5	6	5	6	1	3	4	6	3
строка	2	5	2	1	5	4	3	1	3	3	1	2	1	3	3	3	2	4	1	2
	и	щ	и	в	ы	х	о	д	п	о	д	л	е	с	т	н	и	ц	е	й

49. Юный супергерой перехватил загадочное послание злодея, отправленное его сообщникам: LSB БОРИК ДЕРАР «Теперь-то я знаю, когда они собираются ограбить банк!» – воскликнул супергерой через некоторое время. Извлеките информацию из перехваченного послания и узнайте, какие подробности о плане врага выяснил супергерой.
Ответ: Как догадался супергерой, тайное сообщение содержится внутри текста БОРИК ДЕРАР. При этом пометка LSB указывает, что сообщение скрыто в наименее значимых, т.е. младших, битах (least significant bits), а не в наиболее значимых, т.е. старших, битах (most significant bits, MSB) символов перехваченного текста.
Сопоставим перехваченные символы и соответствующие им двоичные коды: Б – 00001, О – 01110, Р – 10000, И – 01000, К – 01010, Д – 00100, Е – 00101, Р – 10000, А – 00000, Р – 10000.
Предположим, сообщение скрыто в одном младшем бите: Б – 00001, О – 01110, Р – 10000, И – 01000, К – 01010, Д – 00100, Е – 00101, Р – 10000, А – 00000, Р – 10000. Выпишем полученную последовательность: 1000001000. Поскольку двоичные коды представлены пятью битами, разделим полученную последовательность на отдельные последовательности длиной 5 битов: 10000, 01000. Сопоставим этим последовательностям соответствующие символы, согласно приложению: 10000 – Р, 01000 – И. Как видим, осмысленного текста не получилось.
Предположим, сообщение скрыто в двух младших битах: Б – 00001, О – 01110, Р – 10000, И – 01000, К – 01010, Д – 00100, Е – 00101, Р – 10000, А – 00000, Р – 10000. Выпишем полученную последовательность: 01100000100001000000. Разделим полученную последовательность на отдельные последовательности длиной 5 битов и поставим им в соответствие буквы алфавита: 01100 – М, 00010 – В, 00010 – В, 00000 – А. Как видим, осмысленного текста снова не получилось.
Предположим, сообщение скрыто в трёх младших битах: Б – 00001, О – 01110, Р – 10000, И – 01000, К – 01010, Д – 00100, Е – 00101, Р – 10000, А – 00000, Р – 10000. Выпишем полученную последовательность: 0011100000000101001010000000000. Разделим полученную последовательность на отдельные последовательности длиной 5 битов и поставим им в соответствие буквы алфавита: 00111 – З, 00000 – А, 00010 – В, 10010 – Т, 10000 – Р, 00000 – А. Получилось слово «**завтра**», которое является осмысленным и согласуется с исходной ситуацией, описанной в задании.

50. Сумма чисел равна 35. Три умножить на пять будет пятнадцать. Зная это, и то, что длина Великой Китайской стены 21 196 километров, ответьте на следующий вопрос: фпсрыпрвфмкхиеезиэеги?
Ответ: По набору исходных данных (зашифрованный текст и набор цифр) понимаем, что это шифр Цезаря с непостоянным сдвигом или шифр Виженера.
Из цифр в тексте задания составим ключ шифрования: 35351521196.
Так как длина ключа меньше зашифрованного текста, то повторим ключ до достижения необходимой длины. Ключ для каждой буквы – цифра из ключа, стоящая под этой буквой. При расшифровке из номера буквы зашифрованного текста отнимаем ключ. Номер буквы соответствует нумерованному алфавиту из приложения.
Составим таблицу дешифровки.

Шифр-текст	ф	п	с	р	ы	п	р	в	ф	м	к	х	и	е	е	з	и	э	е	г	и
Номер буквы	22	17	19	18	29	17	18	3	22	14	12	23	10	6	6	9	10	31	6	4	10
Ключ	3	5	3	5	1	5	2	1	1	9	6	3	5	3	5	1	5	2	1	1	9
	19	12	16	13	28	12	16	2	21	5	6	20	5	3	1	8	5	29	5	3	1
	с	к	о	л	ь	к	о	б	у	д	е	т	д	в	а	ж	д	ы	д	в	а

Исходный вопрос: сколько будет дважды два? Ответ на него: **четыре**