Министерство образования и науки КР

Гуманитарный колледж КГУ им. И.Арабаева

«Утверждаю»
Директор гуманитарного колледжа
КГУ им. И. Арабаева
Дуйшеналиев Ч.Д.
__ _____ 2022г.

Типовая программа по дисциплине
«Информационная безопасность»

Разработчик (должность) ст. преподаватель
Ф.И.О. Токтогулова Г.А..
Заведующий отделением Информатики и дизайна
Ф.И.О. Турганбаева Б.
Принято на заседании отделения_____.
№ протокола _____
Подпись _____

Рекомендован
Пред. УМС Гум. колледжа
КГУ им. И. Арабаева,
Янгибаева Ж..
(фамилия, И.О.)

«___» _____2022г.

г. Бишкек

Типовая программа

Дисциплины
Информационная безопасность

Направление (специальность) ПОВТАС

Формы обучения очное

Курс 3 Семестр 5

Часов: всего 36, лекций 22, практ. зан. 14,

СРС и виды индивидуальной работы (курсовая работа, проект) ____

Обеспечивающее отделение «Информатика и Дизайн»

Оглавление

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ 4
1.1. Цели и задачи дисциплины 4
1.2. Место дисциплины в структуре образовательной программы 4
1.3. Требования к результатам освоения содержания дисциплины 5
1.4. Объем дисциплины и виды учебной работы 5
1.5. Критерии баллов — рейтинговой оценки знаний и умений студентов. . 6
II. СОДЕРЖАНИЕ ПРОГРАММЫ УЧЕБНОГО КУРСА 10
2.1. Содержание разделов дисциплины ..... **Ошибка! Закладка не определена.**
2.2. Задания для самостоятельной работы студентов ... **Ошибка! Закладка не определена.**
III. ОЦЕНОЧНЫЕ СРЕДСТВА ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ ..... **Ошибка! Закладка не определена.**
3.1. Вопросы к экзамену ..... **Ошибка! Закладка не определена.**
IV. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ 39
4.1. Учебно-методические: основная и дополнительная литература. ..... **Ошибка! Закладка не определена.**
4.2. Интернет-ресурсы ..... **Ошибка! Закладка не определена.**
4.3. Материально — техническое обеспечение дисциплины. ..... **Ошибка! Закладка не определена.**

I. ОРГАНИЗАЦИОННО-МЕТОДИЧЕСКИЙ РАЗДЕЛ

Данная программа предназначена для преподавателей, ведущих данную дисциплину, и для студентов, изучающих дисциплину «Информационная безопасность».

В курсе рассматриваются основные положения информационной безопасности и защиты информации. Рассматриваются основные законодательные акты, касающиеся вопросов информационной безопасности. Вводится понятие информации с точки зрения предмета защиты информации, определяются основные категории, которым должна удовлетворять информация. Вводятся понятие атака на информацию, рассматриваются основные виды атак,последствия от них. Вводится понятие информационная система, информационная сеть, рассматриваются основные виды угроз на них и способы защиты от этих угроз. Для распределенных компьютерных сетей возможные виды угроз передачи информации рассматриваются с привязкой их к уровням модели межсетевого взаимодействия OSI.

1.1. Цели и задачи дисциплины

- привитие навыков обеспечения защиты компьютерных данных.

Задачи преподавания дисциплины: Основными задачами курса является:

- Ознакомить учащихся с видами угроз для информационной безопасности предприятия, организации;
- Ознакомить учащихся с методами обеспечения защиты данных, как на отдельных компьютерах, так и в информационной сети предприятия, организации;
- Ознакомить учащихся с правовыми аспектами информационной безопасности.

.2. Место дисциплины в структуре образовательной программы

Настоящая дисциплина относится к циклу дисциплин профессионального цикла и блоку дисциплин основной программы.

Изучение данной дисциплины базируется на следующих дисциплинах:

-Основы информационной и вычислительной техники

-Информатика

Компетенции, формируемые при изучении дисциплины, необходимы для организации самостоятельной работы студентов, оформления ими докладов и сообщений.

1.3. Требования к результатам освоения содержания дисциплины

В результате освоения ООП выпускник должен обладать следующими компетенциями:

общекультурными:

— способен использовать, обобщать и анализировать информацию, ставить цели и находить пути их достижения в условиях формирования и развития информационного общества (ОК-1);

— способен самостоятельно приобретать и использовать в практической деятельности новые знания и умения, стремится к саморазвитию (ОК-5);

— способен понимать сущность и проблемы развития современного информационного общества (ОК-7);

— способен работать с информацией в глобальных компьютерных сетях (ОК-8).

профессиональными:

— способен использовать основные законы естественнонаучных дисциплин в профессиональной деятельности и эксплуатировать современное электронное оборудование и информационно-коммуникационные технологии в соответствии с целями образовательной программы бакалавра (ПК-3);

1.4. Объем дисциплины и виды учебной работы

Виды учебной работы	**Всего**		**Семестр**
	Часов	Кредиты	5
Аудиторные занятия	36	2	36

Лекционные занятия	22		22
Практические занятия	14		14
Самостоятельная работа	24		24
Вид промежуточной аттестации			Экзамен
Общая трудоемкость часов	60	2	

1.5. Критерии баллов — рейтинговой оценки знаний и умений студентов.

Деятельность студентов в течение семестра оценивается следующим образом: работа на семинарах (50%), самостоятельные работы и реферат (20%), активность (25%), посещение занятий (5%).

Работа на семинарах (50%)

Чтение текстов и участие в дискуссиях являются важными составляющими работы на семинарах. Приветствуются вопросы по структуре и содержанию текста, комментарии, помогающие уяснить значение основных категорий и т.п.

Пропущенные семинары необходимо отработать письменно. «Отработка» должна содержать основные моменты пропущенной темы занятия. Оценка за «отработки» не выставляется. Последний срок сдачи «отработок» - заключительное занятие по курсу (тем, кто не сможет присутствовать на заключительном занятии «отработку» необходимо принести заранее).

Неотработанные семинары являются основанием незачета по данному курсу.

Критерии оценки: регулярное присутствие и активное участие, уместность и глубина вопросов и комментариев, способность задавать живой импульс дискуссии и вовлекать других студентов в дебаты.

Оценки за активность на семинарах выставляются по 10-ти балльной шкале.

Критерии оценки работы студентов на семинарах следующие:

10 баллов – индивидуальный ответ, изложенный по существу структурно, логично, своими словами.

8-9 баллов – индивидуальный ответ, изложенный своими словами. Возможны

мелкие проблемы с логикой изложения.

5-7 баллов – индивидуальный ответ, изложенный частично своими словами. Возможны мелкие проблемы с логикой изложения.

1-4 балла – индивидуальный ответ – уточнение (дополнение) по рассматриваемым вопросам семинарского занятия, задаваемые вопросы.

Самостоятельные работы и реферат (20%)

Самостоятельные работы выполняются на отдельном листочке письменно от руки. Указывается имя, фамилия, группа и дата сдачи работы.

Все письменные работы НЕ принимаются позже установленных сроков сдачи, за исключением документально подтвержденных случаев отсутствия вследствие болезни или форс-мажорных обстоятельств.

Критерии оценки письменных работ следующие:

10 – выдающаяся работа на высоком уровне, присутствует логика и оригинальность изложения, выдвинут и доказан тезис, видно уверенное владение освоенным материалом.

8-9 – очень хорошая работа, продемонстрированы не только усвоенные знания по курсу, но навыки анализа материала и самостоятельного мышления. Возможны мелкие проблемы с логикой изложения.

6-7 – хорошая работа, продемонстрированы не только усвоение фактических знаний по курсу и основные навыки аргументации, но изложение не вполне закончено с точки зрения обоснования тезиса и раскрытия вопроса.

4-5 – средняя работа, неполное усвоение фактических знаний по курсу, слабая логика изложения и обоснования.

2-3 – плохая работа, отрывочные знания по курсу, слабая логика изложения и обоснования.

1 – отсутствие каких-либо знаний.

0 – доказанный случай плагиата.

Темы рефератов студенты выбирают согласно нумерации по учебному журналу.

Реферативная работа оформляется письменно от руки. Допускается печатное

исполнение титульного листа, списка литературы, графических и табличных приложений.

Студенты, вовремя не сдавшие реферат, защищают свою работу на консультации или в дополнительно отведенное время.

Своевременное выполнение работ является предпосылкой к обоснованию возможности допуска студента к зачету (экзамену).

Система оценки знаний

№	Этапы проверки	Вид средства проверки	Баллы	Сроки
1	1 модуль	Тестирование	35	Согласно графику учебного процесса
2	2 модуль	Проверка заданий	35	Согласно графику учебного процесса
3	Практические СРС	Контрольные и графические работы, рефераты, собеседование	10	В течение семестра, до итогового контроля
4	Поощрительные баллы за активность		7	В конце семестра, до итогового контроля
5	Посещение занятий		3	В течение семестра
6	Итоговый контроль	Письменный или	10	Согласно графику учебного процесса

		устный		
	Итого:		**100**	

Штрафные баллы. За пассивное участие в занятиях у студента отнимается из поощрительных баллов штрафные. Если штрафные баллы превышают сумму собранных студентами за семестр поощрительного балла, студент не допускается к сдачи итогового контроля.

Штрафные санкции принимаются так же за не сдачи результатов СРС. В данном случае штрафные баллы больше чем из этой суммы, студент не допускается к сдаче итогового контроля.

Если студент пропускает 3 и более занятий без уважительных причин отстраняется от дисциплины.

Шкала оценки знаний

Процентное содержание (баллы)	Цифровой эквивалент баллов	Оценка по графической системе (по 10 балльной шкале)	Оценка по традиционной системе (4-х балльной)
94,5-100	4,0	A	«5» - отлично
90-94	3,67	A-	
85-89	3,33	B+	
80-84	3,0	B	«4» - хорошо
75-79	2,67	B-	
70-74	2,33	C+	
65-69	2,0	C	«3» - удовлетворительно
60-64	1,67	C-	
55-59	1,33	D+	
50-54	1,0	D	

0-49	0	F	Неудовлетворительно
X	X	X	Студент отстранен от дисциплины

II. СОДЕРЖАНИЕ ПРОГРАММЫ УЧЕБНОГО КУРСА

2. Тематический план

№	Наименование тем	часы	
		лк	пр
Модуль 1			
1	Тема 1. Информация как объект защиты. Законодательные основы по защите информации.	1	
2	Тема 2. Защита информации в персональном компьютере. Особенности защиты информации в персональном компьютере. Программные средства защиты информации.	3	2
3	Тема 3. Угрозы информационной системы (случайные, преднамеренные воздействия).	2	2
4	Тема 4. Информационные компьютерные сети. Удаленные атаки. Особенности защиты информации в компьютерных сетях.	2	2
5	Тема 5. Стандарты и спецификации в области информационной безопасности.	2	1
	итого	10	7
Модуль 2			
6	Тема 6. Обзор аппаратно-программных средств защиты информации.	2	1

7	Тема 7. Обзор модели межсетевого взаимодействия OSI. Уровни сетевых атак согласно модели OSI	2	
8	Тема 8. Предмет и задачи криптографии и криптоанализа.	2	
9	Тема 9. Симметричные системы шифрования.	2	3
10	Тема 10. Ассиметричные системы шифрования.	2	3
11	Тема 11 Проблема вирусного заражения и структура современных вирусов.	1	
12	Тема 12. Классификация антивирусных программ.	1	
	Итого	12	7
	Всего	22	14

Тематика самостоятельной работы студентов

№	Наименование тем	Формы контроля	
1	Борьба с угрозами несанкционированного доступа к информации	презентация	
2	Актуальность проблемы обеспечения безопасности информации.	Устный опрос	
3	Виды мер обеспечения информационной безопасности.	Создание карточек в StudyStack	
4	Защита информации в персональном компьютере	презентация	
5	Особенности защиты информации в персональном компьютере.	Устный опрос	
6	Программные средства защиты информации.	Письменная работа	
7	Криптографические методы защиты информации.	Создание проекта в Padlet	
8	Криптология и основные этапы ее развития.	Письменная работа	
9	Методы криптографических преобразований.	презентация	

10	Стандарты шифрования.	Письменная работа	
11	Борьба с вирусным заражением информации	презентация	
12	Проблема вирусного заражения и структура современных вирусов	Создание проекта в Padlet	
13	Классификация антивирусных программ	Создание проекта в Padlet	

Содержание практических работ

ПРАКТИЧЕСКИЕ РАБОТЫ

Симметричные криптосистемы

Симметричные алгоритмы или алгоритмы шифрования с одним ключом используют для шифрования и дешифрования один и тот же ключ. В этом разделе рассматриваются простейшие алгоритмы шифрования, представляющие принципиальную основу современных компьютерных алгоритмов шифрования.

3.1.1 Шифры перестановки

В шифрах средних веков часто использовались таблицы, с помощью которых выполнялись простые процедуры шифрования, основанные на перестановке букв в сообщении. Ключами в этих алгоритмах являются размеры таблицы и порядок перестановки. Пример данного метода шифрования текста «**И БУМАЖКОЙ ПРИКРОЕМ БРЕШЬ**» показан в таблицах на рис 3.1. Сначала в таблицу записывается текст сообщения (рис 3.1, а), а потом поочередно переставляются столбцы в определенном порядке (на рис 3.1, б) в первой строке, а затем строки (на рис 3.1, в) в последнем

столбце. При расшифровке порядок перестановок был обратный. Пример данного метода шифрования показан в следующих таблицах:

Рис. 3.1. Двойная перестановка столбцов и строк

В результате перестановки текста «**И БУМАЖКОЙ ПРИКРОЕМ БРЕШЬ**» получена шифровка «**ИП РКМОРЕ ШРБЕЬОЖАКЙУ ИБМ**». Ключом к шифру служат номера столбцов 4 2 1 3 5 и номера строк 3 4 5 2 1 исходной таблицы.

Для удобства запоминания ключей можно использовать в их качестве слова. При этом порядок перестановки определяется нумерацией букв в слове в алфавитном порядке. В приведенном примере использованы *Ключ1* – «СПОРТ», буквы в алфавите располагаются в порядке 4 2 1 3 5 (ОПРСТ – 12345) и *Ключ2* – «СТУЖА», буквы в алфавите располагаются в порядке 3 4 5 2 1 (АЖСТУ–12345). Число вариантов двойной перестановки достаточно быстро возрастает с увеличением размера таблицы: для таблицы 3 x 3 их 36, для 4 x 4 их 576, а для 5 x 5 их 14400.

Для обеспечения дополнительной защиты можно повторно шифровать сообщение, которое уже было зашифровано. Для этого размер второй таблицы подбирают так, чтобы длины ее строк и столбцов отличались от длин строк и столбцов первой таблицы. При этом размеры второй таблицы должны быть взаимно простыми с размерами первой таблицы.

Для шифрования применялись магические квадраты – квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная с единицы, которые дают в сумме по каждому столбцу,

каждой строке и каждой диагонали одно и то же число. Свойство магического квадрата используется для повышения эффективности шифра при данном алгоритме шифрования. Для шифрования необходимо вписать исходный текст «ЧИСЛОШЕСТНАДЦАТЬ» по приведенной в магическом квадрате нумерации и затем переписать содержимое таблицы по строкам (рис 3.2). В результате получается шифротекст «ЬСИЦОНАСТШЕДЛТАЧ», сформированный благодаря перестановке букв исходного сообщения.

Исходный текст: Ч И С Л О Ш Е С Т Н А Д Ц А Т Ь

Ч	И	С	Л	О	Ш	Е	С	Т	Н	А	Д	Ц	А	Т	Ь
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16

Магический квадрат

16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

Шифрование

Ь	С	И	Ц
О	Н	А	С
Т	Ш	Е	Д
Л	Т	А	Ч

Шифротекст: Ь С И Ц О Н А С Т Ш Е Д Л Т А Ч

Рис. 3.2. Шифрование с помощью магического квадрата

Дешифровка шифротекста происходит в обратном порядке: вначале текст вписывается последовательно слева направо в квадрат, затем буквы с квадрата выбираются в порядке, определенном в магическом квадрате.

3.1.2 Шифры простой замены

Шифры простой замены использовались еще в древней Греции (V–VI до н.э.), которые и в настоящее время являются частью отдельных алгоритмов шифрования.

Система шифрования Цезаря – частный случай шифра простой замены. Метод основан на замене каждой буквы сообщения на другую букву того же алфавита, путем смещения от исходной буквы на К букв.

Известная фраза Юлия Цезаря VENI VINI VICI – пришел, увидел, победил, зашифрованная с помощью данного метода, преобразуется в SBKF SFAF SFZF (при смещении на 4 символа).

Греческим писателем Полибием за 100 лет до н.э. был изобретен так называемый *квадрат Полибия* размером 5 x 5, заполненный алфавитом в случайном порядке. Греческий алфавит имеет 24 буквы, а 25-м символом является пробел. Для шифрования на квадрате находили букву текста и записывали в шифротекст букву, расположенную ниже ее в том же столбце. Если буква оказывалась в нижней строке таблицы, то брали верхнюю букву из того же столбца.

3.1.3 Шифры сложной замены

Шифр Гронсфельда состоит в модификации шифра Цезаря числовым ключом. Для этого под буквами сообщения записывают цифры числового ключа. Если ключ короче сообщения, то его запись циклически повторяют. Шифротекст получают примерно также, как в шифре Цезаря, но отсчитывают не третью букву по алфавиту (как в шифре Цезаря), а ту, которая смещена по алфавиту на соответствующую цифру ключа.

Пусть в качестве ключа используется группа из трех цифр – 314, тогда сообщение «**ТРУДНО В УЧЕНИИ**» преобразуется в шифрограмму «**ХСШЖОТВГГЧШИРКН**» (рис. 3.3).

Сообщение	**Т Р У Д Н О В У Ч Е Н И И**
Ключ	**3 1 4 3 1 4 3 1 4 3 1 4 3 1 4**
Шифровка	**Х С Ш Ж О Т В Г Г Ч Ш И Р К Н**

Рис. 3.3. Реализация шифра Гронсфельда

В *шифрах многоалфавитной замены* для шифрования каждого символа исходного сообщения применяется свой шифр простой замены (рис. 3.4).

	АБВГДЕЁЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_
А	АБВГДЕЁЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_
Б	_АБВГДЕЁЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ
В	Я_АБВГДЕЁЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮ
Г	ЮЯ_АБВГДЕЁЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭ
.	.....
Я	ВГДЕЁЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_АБ
_	БВГДЕЁЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ_А

Рис. 3.4. Таблица для реализации шифра многоалфавитной замены

Сообщение	Э К С П Е Р И М Е Н Т
Ключ	Б А Б А Я Г А Б А Б
Шифровка	Ь К Р П Ё Т Ё М Д Н С

Рис. 3.5. Пример реализации шифра многоалфавитной замены

Каждая строка в этой таблице соответствует одному шифру замены аналогично шифру Цезаря для алфавита, дополненного пробелом. При шифровании сообщения его выписывают в строку, а под ним ключ. Если ключ оказался короче сообщения, то его циклически повторяют. Шифротекст получают, находя символ в колонке таблицы (рис 3.4) по букве текста и строке, соответствующей букве ключа. Например, используя ключ «БАБА ЯГА», из сообщения «ЭКСПЕРИМЕНТ» получаем следующую шифровку «ЬКРПЁТЁМДНС».

Такая операция с использованием таблицы, приведенной на рис 3.4, соответствует сложению кодов ASCII символов сообщения и ключа по модулю равным числу символов.

3.1.4 Гаммирование

Процесс шифрования заключается в генерации гаммы шифра (ключа) и наложении этой гаммы на исходный открытый текст. Перед шифрованием открытые данные разбиваются на блоки $T(0)_i$ одинаковой длины (например, по 64 бита). Ключ шифра (гамма шифра) вырабатывается в виде последовательности блоков $Г(ш)_i$ аналогичной длины, шифротекст $T(ш)_i=Г(ш)_i+T(0)_i$, где «+» – побитовое сложение, $i=1,2,...,m$. Процесс дешифрования сводится к повторной генерации шифра текста и наложение этой гаммы на зашифрованные данные, т.е. $T(0)_i=Г(ш)_i+T(ш)_i$. Алгоритмы гаммирования легко реализуются на компьютере и, как правило, являются частью симметричных алгоритмов криптографии.

3.2 Задания для выполнения

3.2.1 Используя алгоритмы двойной перестановки строк и столбцов выполнить шифрование следующих фраз (ключ выбирать самостоятельно, номер варианта выбрать по номеру в списке группы):

1. Он досрочно завалил экзамен.
2. Закон суров, но это закон.
3. Умному легче доказать, что он дурак.
4. И у дурака вырастает зуб мудрости.
5. Свободу симулировать нельзя.
6. Подумай, прежде чем подумать.
7. Каждый век имеет свое средневековье.
8. Брюки протираются даже на троне.
9. Окно в мир можно закрыть газетой.

10. Чаще всего выход там, где был вход.
11. Безграмотные вынуждены диктовать.
12. Хлеб открывает любой рот.
13. Деньги не пахнут, но улетучиваются.
14. Сны зависят от положения спящего.
15. Труднее всего поджечь ад.
16. Ужасен кляп, смазанный медом.
17. Не пиши кредо на заборе.
18. Беззубым многое легче выговаривать.
19. И регалии звенят по разному.
20. Лицемерный палач ослабляет петлю.
21. Интеллектуальная узость ширится.
22. Вписывайся во влиятельные круги.
23. Иные ступени карьеры ведут на виселицу.
24. И маятник идет в ногу со временем.
25. И ненужные постоянно нужны.

3.2.2 Используя алгоритмы двойной перестановки строк и столбцов выполнить дешифрование шифрограмм, приведенные в таблице 3.1 (номер варианта выбрать по последней цифре номера шифра). В шифротексте следует обратить внимание на наличие пробелов в тексте, длина текста по всем вариантам равняется 25 символам:

Таблица 3.1

Номер вар-та	Шифротекст	Ключ 1	Ключ 2
1	**В ОН, Т ОЭЗКНОА УОРСЗКНОА**	КРУТО	СТУЖА
2	**ЗВАОЛИ ЛАН ОДОРОНЧСАЧТЕЗ**	ВЕСНА	ОСЕНЬ

3	ПАЙРДЕЕЖ М ЧЕДАТУМЬДУПОМ	ОСЕНЬ	ДОСУГ
4	ДОВХЫМА Т ЕД Г ДО ХВ ИИЩ	ТРАВА	ДОСУГ
5	!Т РОЙОЛЮБ БХЛЕ ТВАЕЫРОТК	ПРАВО	ТРАВА
6	Ь ДА ОЖЧЕДТУНДРЕ СВЕЕОП Г	КРУТО	ПРАВО
7	ЕН ПОЕРД ЕОБР!ЗАН А ШИИК	СПОРТ	КРУТО
8	Е ВГОБЫ-М БЕУЗЗ ЛЧЕГОРЬИТ	ВЕТЕР	СПОРТ
9	ГАЛЕР ЗВИИОМУНЗЯТ НЕ РАОП	СТУЖА	ВЕТЕР
10	СЯТООН ОН УЫЖННЫПЕН ЕЖННУ	ДРЕВО	СТУЖА

3.2.3 Используя магический квадрат (таблица 3.2) расшифровывать следующие шифрограммы (шифрограммы приведены в таблице 3.3, номер варианта выбрать по числу букв в фамилии):

Таблица 3.2

11	24	7	20	3
4	12	25	8	16
17	5	13	21	9
10	18	1	14	22
23	6	19	2	15

Таблица 3.3

Вариант	Шифротекст
1	ОЛ ЕЛ ОДУЛА-СЕЛЯС МЕЛЙДГ
2	ВТТЙЕБА КЛЮ Е РЫБХТРОООЛ
3	ОЕР Д ТОАЛОЗЗЧНИОААЧСЛНВ
4	УЗУНОБЛЯСВАОИЕИМТСРЛЬДЬВО
5	ЕТЙДДУЖЬ ЧЕМДУПРМПЕМАА О
6	ЕАЕЕУДГД ПОНОЧВСДТ Ь ЕЖР
7	КРШЗ РЕИ НПЕА АНДБОИ ЕО
8	ОНЫ НУСЫЕННЖТН ПОНОУЖН ЕЯ
9	ЕМИАГАНУ ПОЛЯЗЗВ РТНОИРЕ
10	НУУ З Е!ДЛЬТ РА КБТЫБРОЕО

3.2.4 Используя шифр многоалфавитной замены шифровать фразу из п. 3.2.1 (исключив пробелы и знаки препинания), используя в качестве ключа «Ключ 1» из пункта 3.2.2. Для шифрования использовать алфавит замены из таблицы 3.5.