Титульный лист программы дисциплины (SYLLABUS)

Форма
Ф СО ПГУ 7.18.4/19

**Министерство образования и науки Республики Казахстан**

**Павлодарский государственный университет им. С. Торайгырова**

**Кафедра Вычислительная техника и программирование**

# ПРОГРАММА ДИСЦИПЛИНЫ (SYLLABUS)

Основы информационной безопасности

Павлодар, 2013 г.

Лист утверждения программа дисциплины (Syllabus)

Форма
Ф СО ПГУ 7.18.4/19

**УТВЕРЖДАЮ**
Декан факультета ФМиИТ
_____ Испулов Н.А.
(подпись) (Ф.И.О.)
«___»_____20__г.

Составитель: ст. преподаватель _____Ахмерова З.Р.
(должность, учёная степень, звание, подпись) (Ф.И.О.)

# Программа дисциплины (Syllabus)

Основы информационной безопасности OIB 3302
(полное наименование и код дисциплины по рабочему учебному плану)
для студентов очной формы обучения специальности(ей)
(форма обучения)
5В070400 Вычислительная техника и программное обеспечение
(шифр и полное наименование специальности (ей))

Программа разработана на основании рабочей учебной программы, утверждённой «___» _____20__г.

Рекомендована на заседании кафедры от «___»_____20__г.
Протокол №_____.
Заведующий кафедрой _____ Потапенко О.Г. «__»_____20__г.
(подпись) (Ф.И.О.)

Одобрена учебно-методическим советом ФМиИТ факультета
(наименование факультета)
«____»_____20__г. Протокол №____

Председатель УМС ____ Искакова А.Б. «____» _____20__г.
(подпись) (Ф.И.О.)

## 1. Паспорт учебной дисциплины

**Наименование дисциплины** Основы информационной безопасности

**Количество кредитов и сроки изучения**
Всего – 3 кредита
Курс: 1, 3
Семестр: 2, 6

Всего аудиторных занятий – 52,5 часов
Лекции -15
Практические /семинарские занятия -22,5 часов
Лабораторные –15
СРС – 82,5 часов, в том числе СРСП – 20,625 часов
Общая трудоемкость - 135 часов

**Форма контроля**
Курсовая работа – 2 (1 курс), 6 (3 курс) семестр
Форма итогового контроля: Экзамен – 2 (1 курс), 6 (3 курс) семестр

**Пререквизиты**
Для освоения данной дисциплины необходимы знания, умения и навыки приобретенные при изучении следующих дисциплин: «Высшая математика»; «Информатика»; «Программирование на языке высокого уровня (Delphi 6, 7; Borland – Pascal 7.0)»

**Постреквизиты**
Знания, умения и навыки, полученные при изучении дисциплины необходимы для освоения следующих дисциплин: «Компьютерные сети», «Интернет технологии».

## 2. Сведения о преподавателях и контактная информация

Ф.И.О. Ахмерова Зарема Равильевна
Учёная степень, звание, должность старший преподаватель
*Научные, методические и другие достижения (по желанию разработчиков)*

Кафедра «ВТиП», аудитория А-403
E-mail: Ahmerova_Zarema@mail.ru

## 3. Предмет, цели и задачи

**Предмет дисциплины** Основы информационной безопасности

**Цель преподавания дисциплины**

изучение студентами теоретических основ и методов защиты информации, математической структуры секретных систем, рассмотрение математического представления информации, методов анализа информационных характеристик и избыточности языковых систем, теоретических основ коррекции и восстановления информационных характеристик произвольных текстов, построение систем защиты информации, освоение основных методов и средств защиты информации.

**Задачи изучения дисциплины**

- изучение и освоение:
- источников и форм атак на информацию;
- моделей безопасности (в том числе, основных операционных систем);
- разновидностей вредоносных программ;
- криптографических и административных методов защиты;
- администрирование корпоративных и локальных сетей, методы защиты сетей и протоколов;

- алгоритмов аутентификации пользователей.

## 4. Требования к знаниям, умениям, навыкам и компетенциям

В результате изучения дисциплины студенты должны

иметь представление:

- о методах и средствах защиты информации;

знать:

- определение и основные информационно-статические характеристики языковых систем;
- математическое представление секретных систем;
- методы анализа текстов и определение их избыточности;
- методы построения систем трансформации информационно-статических характеристик текстов;
- практические способы построения систем защиты информации;

уметь:

- анализировать тексты и определять их избыточность;
- разрабатывать системы трансформации информационно-статистических характеристик текстов;
- разрабатывать системы защиты информации;
- подбирать и применять методы защиты информации;
- подбирать и применять средства защиты информации.

## 5 Тематический план изучения дисциплины

### Распределение академических часов по видам занятий

| Форма обучения | Трудоемкость дисциплины | | | | Формы контроля по семестрам | | | | Семестр | Объем работы студентов по семестрам | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | кредитов | академических часов | | | | | | | | кредитов | аудиторных занятий (ак. часов) | | | | СРС (ак. часов) |
| | | всего | ауд | СРС | экз. | зач. | КП | КР | | | всего | лек | пр. | лаб | всего |
| очная на базе ОСО 2011 | 3 | 135 | 52,5 | 82,5 | 6 | | | 6 | 6 | 3 | 52,5 | 15 | 22,5 | 15 | 82,5 |

## 6. Содержание лекционных занятий

**Тема 1** Введение. Защита информации

Понятие национальной безопасности. Виды безопасности: государственная, экономическая, общественная, военная, экологическая, информационная. Роль и место системы обеспечения информационной безопасности в системе национальной безопасности. Информационные угрозы. Противодействие информационным угрозам. Характеристические свойства систем защиты информации. Методы защиты информации. Предмет защиты. Средства защиты. (1-3)

**Тема 2** Безопасность информации

Характеристические свойства систем обеспечения безопасности информации. Методы обеспечения безопасности информации. Средства обеспечения безопасности информации. (1-3)

**Тема 3** Анализ программной и аппаратной платформы информационных систем

Архитектура электронных систем обработки данных. Архитектура программного обеспечения. Системные средства обработки данных. Прикладные средства обработки данных. Аппаратные средства информационной защиты. Программные средства информационной защиты. (1-3)

**Тема 4** Модели безопасности информационных систем

Формальные модели. Модели безопасности. Политика безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Стандарты по оценке защищенных систем. (1-3)

**Тема 5** Примеры практической реализации систем защиты и безопасности

Построение парольных систем; особенности применения криптографических методов. Способы реализации криптографической подсистемы; особенности реализации систем с симметричными и несимметричными ключами; способы реализации стенографических систем. (1-3)

**Тема 6** Основные характеристики защищенной информационной системы

Концепция защищенного ядра. Методы верификации. Защищенные домены. Применение иерархического метода для построения защищенной операционной системы. (1-3)

**Тема 7** Методология корректности информационной защиты

Исследование корректности систем защиты; методология обследования и проектировании защитных механизмов; модель политики контроля целостности. (1-3)

**Тема 8** Мера защиты информации

Определение необходимой меры защиты информационных ресурсов; методы оценки меры защиты информации; основные показатели оценки уровня защиты информации; характеристики мер защиты. (1-3)

**Тема 9** Оптимальное управление процессами защиты

Модели и методы оптимального управления процессами обеспечения безопасности при:

- проектирование аппаратных средств защиты;
- проектирование программных средств защиты;
- проектирование организационных мер защиты. (1-3)

**Тема 10** Оценка системы защиты

Комплексная оценка системы защиты информации. Тестирование программного обеспечения. Проблема тестирования программных продуктов, автоматическое тестирование, принципы написания самотестирующихся программных продуктов. Инсталляция тестов в готовые программные продукты Оценка надежности защитных механизмов. Принципы оценки надежности защиты. (1-3)

**Тема 11** Безопасность компьютерных систем

Защита в локальных сетях. Программные средства индивидуальной защиты информации. Использование экспертных систем для распознавания попыток несанкционированного доступа. (1-3)

## 7. Содержание практических (семинарских, лабораторных, студийных, индивидуальных) занятий, их объем в часах

**Тема 1.** Методы шифрования данных. Метод Цезаря.

План занятия:

1. Разработать универсальный программный продукт, реализующий шифрование данных, используя метод Цезаря.
2. Разработать универсальный программный продукт, реализующий дешифрование данных, используя метод Цезаря.
3. Выполнить индивидуальное задание, согласно своему варианту, и оформить результаты работы в виде отчета.

Контрольные вопросы:

1. Алгоритм шифрования данных.
2. Алгоритм дешифрования данных.
3. Требования к ключу.

Методические рекомендации по выполнению задания:

**Теоретические сведения**

Самым древним и самым простым из известных подстановочных шифров является шифр, использовавшийся Юлием Цезарем. В шифре цезаря каждая буква алфавита заменяется буквой, которая находится на три позиции дальше в этом же алфавите. При этом алфавит считается «циклическим», т.е. за буквой Я следует буква А. Например, для алфавита

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

шифрование происходит следующим образом:

Открытый текст: К Р И П Т О Г Р А Ф И Я

Шифрованный текст: Н У Л Т Х С Ж У Г Ч Л В

Определить преобразование можно, перечислив все варианты, как показано ниже.

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

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

Если каждой букве назначить числовой эквивалент (А = 1, Б = 2 и т.д.), то алгоритм шифрования можно выразить следующими формулами. Каждая буква открытого текста *P* заменяется буквой шифрованного текста *C*:

$$C = E(P) = (P+3) \bmod (26).$$

В общем случае сдвиг может быть любым, поэтому общий алгоритм Цезаря записывается формулой

$$C = E(P) = (P+k) \bmod (26),$$

где *k* принимает значения в диапазоне от 1 до 31 (для рассмотренного алфавита). Алгоритм дешифрования также прост:

$$P = D(C) = (C-k) \bmod (26).$$

Если известно, что определенный текст был зашифрован с помощью шифра Цезаря, то с помощью простого перебора всех вариантов раскрыть шифр очень просто – для этого достаточно проверить 31 возможный вариант ключа.

Применение метода последовательного перебора всех возможных вариантов оправдано следующими тремя важными характеристиками данного шифра.

1. Известны алгоритмы шифрования и дешифрования.
2. Необходимо перебрать всего 31 вариант.
3. Язык открытого текста известен и легко узнаваем.

В большинстве случаев, когда речь идет о защите компьютерной информации, можно предполагать, что алгоритм известен. Единственное, что делает криптоанализ на основе метода последовательного перебора практически бесполезным – это применение алгоритма, для которого требуется перебрать слишком много ключей.

При наличии всего 31 возможного варианта ключей шифр Цезаря далек от того, чтобы считаться надежно защищенным. Существенного расширения пространства ключей можно добиться, разрешив использование произвольных подстановок.

Например, если в шифре Цезаря допустить использование любой из перестановок 31 символа алфавита, а не только сдвигом на *k* символов, то мы получим 31! Возможных ключей. Пример ключа такого шифра приведен ниже.

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

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

Пример шифрования с использованием этого ключа:

Открытый текст: К Р И П Т О Г Р А Ф И Я

Шифрованный текст: Ф Ю В Ч Ц С Ь Ю Й Э В З

Создается впечатление, что 31! (что превышает $8\times10^{33}$) ключей не так то просто перебрать, и данный шифр обладает высокой степенью надежности. Однако для криптоаналитика существует и другая линия атаки. Если криптоаналитик имеет представление о природе открытого текста (например, о том, что это текст на английском языке), можно использовать известную информацию о характерных признаках, присущих текстам на соответствующем языке.

**Варианты индивидуальных заданий**

По возможности дешифратор должен быть универсальным, то есть работать с неопределённым ключом, и выводить единственно верный результат.

Имеется шифрованный текст (смотрите таблицу), полученный с помощью шифра Цезаря. Величина используемого при этом сдвига неизвестна. Расшифруйте сообщение.

| Вариант | Задание |
|---|---|
| 1. | ИЦРХЭЫЩШШЩРЫЩЩМДРШУРМЮПРЭЪЩЬЭРЪРШШЩТЛЧ РШКЭЗЩМЖВШЩРМЮЧЛСШЩРЫЩЩМДРШУР |
| 2. | ФГМКРОНФЩЗТЪЦФЫКШНФНХРТЦЛМИЩЪШИХГЙЫМЫЪЧНШНЩН ЯНХГЩНЪЗФРЧНШНМИЯРМИХХГЭ |
| 3. | ВЦЫБЦГЮМЦСФЦЮГВГУСЩЭЦПГХЯВГДАЫЖЯБЯЙЦЪЫБЩАГЯФБСЕ ЩИЦВЫЯЪГЦЖЮЯЬЯФЩЩ |
| 4. | КЭЧУЙЧБЗЪАДЮНЮКБИЭКЗШФДЙНОЮБМЬЙББЙБДИБЗДАКНОПЛЬЖЖ МДЛОКЯМЬРДУБНЖДИОБСЙКЗКЯДЫИЮКБЙЙКЯКПМКЮЙЫ |
| 5. | ТБВРЭФРАВЭЛЕЪАШЯВЮУАРДШЗХБЪШЕБШБВХЬРЕШБЯЮЫМЧГХВБП ЮФШЭШВЮВЦХЪЫОЗШФЫПИШДАЮТРЭШПШФЫПАРБИШДАЮТЪШ |
| 6. | ШАЖЮЕИДЩЖЦКЮНЫЗАДЯЗЮЗИЫВЫЗДИАЖСИСВАБФНДВАЦЬЪСЯЮ ВЫЫИЪШЦЗШХЭЦГГСЛШЭЦЮВГДАБФНЦ |
| 7. | ШОФТЙЧШЩМЕТУЖЦВЮБУАШЬТ,ЯТУЩОЫЫЙЧЯЭЬЪЬЗКМТЮБСЬСЬ ШЩМЕО |
| 8. | ПМЯПРАГЛЛЩЗПГИОГРЛЩЗИЙЬХМРНОЮАЖРГЙЭКМДГРЯЩРЪЖПНМЙ ЪЕМАЮЛВЙЭЦЖТОМАИЖПММЯЧГЛЖЭ |
| 9. | ЙЧСЦЮЬЪЩЩМЛЫЪРЫФЭИЭЪЪНЕСЩФЛРЪЦМУЗОМСЮГЮЪЪЮЫЬМО ФЮСЧСШНЗЧРСХЭЮОФЮСЧИЩЪЭЪУРМЮСЧИЭЪЪНЕСЩФЛ |
| 10. | ЖКВИУКУЭВГЦПАНИШЕЧКЙЧЪЪАЬЭЙЭИКАМАВШКЖЪВГЦПЭБВЖКЖ ИУЭЪВГЦПШЦКЪЙЭЩЧАЬЭЕКАМАВШКЖИЗЖГФЯЖЪШКЭГЧ |

Рекомендуемая литература (2, 5, 6)

**Тема 2.** Методы шифрования данных. Метод «Лесенка».

План занятия:

1. Разработать универсальный программный продукт, реализующий шифрование данных, используя метод «Лесенка».
2. Разработать универсальный программный продукт, реализующий дешифрование данных, используя метод «Лесенка».

3. Выполнить индивидуальное задание, согласно своему варианту, и оформить результаты работы в виде отчета.

Контрольные вопросы:

1. Алгоритм шифрования данных.
2. Алгоритм дешифрования данных.
3. Требования к ключу.

Методические рекомендации по выполнению задания:

**Теоретические сведения**

Шифры, созданные с помощью перестановок, называют *перестановочными* шифрами.

Простейший из таких шифров использует преобразование «лесенки», заключающейся в том, что открытый текст записывается вдоль наклонных строк определенной длины («ступенек»), а затем считывается построчно по горизонтали. Например, чтобы шифровать сообщение «шифр с использованием перестановки» по методу лесенки со ступеньками длиной 2, запишем это сообщение в виде

Ш Ф С С О Ь О А И М Е Е Т Н В И
И Р И П Л З В Н Е П Р С А О К

Шифрованное сообщение будет иметь следующий вид.

ШФССОЬОАИМЕЕТНВИИРИПЛЗВНЕПРСАОК

**Варианты индивидуальных заданий**

По возможности дешифратор должен быть универсальным, то есть работать с неопределённым ключом, и выводить единственно верный результат.

К открытому тексту был применен шифр «Лесенка». Восстановите сообщение по шифрованному тексту из таблицы.

| Вариант | Задание |
|---|---|
| 1. | ВЩИТЗЬВЬЛОНЕНИУШИЗЕГАЕТСЮЕНОЙОСВЕПТПЫВЗШТРРОБОПАЕАО МНЛОЛОТМРЯЯЕЬЛОЛЕНА |
| 2. | ЛЕСЕПЕУЕОНЬНЯПЗННМИЬУИЩЮДТКРТЮБПОХЕИООИФАЕНШЕИБЕВО ОИЩЕАСРНИЛВЯОЦСАЕЗТОЙИММРЕЗСТАИСЬАИРИТРНАЫ |
| 3. | МЕЕЕСНЬМТПЦСНРЧЯТЫЗДОЕЕТОЫЕТИСООВЧЛИГЧСЕСИВКИЕОИЕКЛВ САУОНСЕЛОЬЯПНМБИТСОЙНЗОИЕЕЕНФВДОАЛЕНСМО |
| 4. | ВРОСМЕННАЗАРТМНММММИМНИАКНФЦЯСОВУЕАДЕНАНСХТАОИЛЕЛО ЮЕЖОНФЦЫТЭРЯРЯАБЬДРБНКТОИХЕЛОИМВНЯОИАУЫУА |
| 5. | САААИАЕЬДЛЬЩКТСЕМИБСДОЧКЕЬХЕОЕИИАСЕНОБИОННРЙМРСНЦТЗОЛ ЕВНЦОАСПНТФИЕОСЖСАФИСНЯЬОЕОИМПТНПТИАТЯВЮЙМР |
| 6. | ОЗСЗСЕСЕОИИИЩДАТОТТПНЙФИКЕНДЕПИСЕАИИСАНОАМАЯЯЧДДКТС ИЙЧЫСВОЕЕЕАООЯИСБНЛЬНЖНЦЧОЗИЕОЯЕИНТИНЬ |
| 7. | СЕЕАСБЕАЕМООЧЯРТОКЕАОЕИМЗСТЕЧЕВОСТЕОАЕТТРЧОНСАОНИСИТО ЖТРНТВЛФАЕИБИТБПООПВНЗНЬЕИПИЯАПДСЩЯ |
| 8. | ОИЯИОРИОМТБЕДННСТРЕВЕКОФНАЬОШАСОСОЫМОНАПНТРМИТНТЕТ УМРЗПЕЕЧРПАЕБОГЛЕОАЦСАСОЬНЛКИУВТВС |
| 9. | ПВАНЩОАЕИНРИЫЯТЗТЫАНРИИСРРТГЕДХВСРЕМСЫУЯТЯАМОАДАИЛЯУ ЛИСЕШЗЫТКОРПАННЯРШЬИНЕАНХТНИЕЧНЕЮАИН |
| 10. | КЕЬИАНЗПДООИАЕИООННЦАААОАТЖЕЛССВНЦОФИЧЩТНВНГИКСАФИС ОИАИОНОООТОЛНИАТРОЕТКЫЗСАИГЕИДЛЬМЗТУАХМТНЧОДЯ |

Рекомендуемая литература (2, 5, 6)

**Тема 3.** Методы шифрования данных. Метод Виженера.

План занятия:

1. Разработать универсальный программный продукт, реализующий шифрование данных, используя метод Виженера.

2. Разработать универсальный программный продукт, реализующий дешифрование данных, используя метод Виженера.

Контрольные вопросы:

1. Алгоритм шифрования данных.
2. Алгоритм дешифрования данных.
3. Требования к ключу.

Методические рекомендации по выполнению задания:

**Теоретические сведения**

Другая возможность усовершенствования простого моноалфавитного шрифта заключается в использовании нескольких моноалфавитных подстановок, применяемых в ходе шифрования открытого текста в зависимости от определенных условий. Семейство шрифтов, основанных на применении таких методов шифрования, называется *полиалфавитными шифрами.* Подобные методы шифрования обладают следующими общими свойствами.

1. Используется набор связанных моноалфавитных подстановок.
2. Имеется некоторый ключ, по которому определяется, какое конкретное преобразование должно применяться для шифрования на данном этапе.

Самым широко известным и одновременно самым простым алгоритмом такого рода является шифр Виженера (Vigenure). Этот шифр базируется на наборе правил моно алфавитной подстановки, представленных 26 шифрами Цезаря со сдвигом от 0 до 25 (для латинского алфавита). Каждый из таких шифров можно обозначить ключевой буквой, являющейся буквой шифрованного текста, соответствующего букве A открытого текста. Например, шифр Цезаря, для которого смещение равно 3, обозначается ключевой буквой D.

Для облегчения понимания и применения этой схемы была предложена матрица, названная «табло Виженера» (см. табл. 1). Все 26 шифров располагаются по горизонтали, и каждому из шифров соответствует своя ключевая буква, представленная в крайнем столбце слева. Алфавит, соответствующий буквам открытого текста, находится в первой сверху строке таблицы. Процесс шифрования прост – необходимо по ключевой букве $\boldsymbol{x}$ и букве открытого текста $\boldsymbol{y}$ найти букву шифрованного текста, которая находится на пересечении строки $\boldsymbol{x}$ и столбца $\boldsymbol{y}$. В данном случае такой буквой является буква *V*.

Таблица 1. Табло Виженера.

| | **a** | **b** | **c** | **d** | **e** | **f** | **g** | **H** | **i** | **j** | **k** | **l** | **m** | **n** | **o** | **p** | **q** | **R** | **s** | **t** | **u** | **v** | **w** | **x** | **y** | **z** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **a** | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| **b** | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| **c** | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| **d** | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| **e** | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| **f** | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| **g** | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| **h** | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| **i** | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| **j** | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| **k** | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| **l** | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| **m** | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| **n** | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| **o** | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| **p** | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| **q** | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| **r** | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| **s** | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| **t** | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| **u** | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| **v** | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| **w** | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| **x** | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| **y** | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| **z** | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

Чтобы зашифровать сообщение, нужен ключ, имеющий туже длину, что и само сообщение. Обычно ключ представляет собой повторяющееся нужное число раз ключевое слово, чтобы получить строку подходящей длины. Например, если ключевым словом является *deceptive*, сообщение «we are discovered save yourself» шифруется следующим образом:

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Открытый текст: | D | E | C | E | P | T | I | V | E | D | E | C | E | P | T | I | V | E | D | E | C | E | P | T | I | V | E |
| Ключ: | W | E | A | R | E | D | I | S | C | O | V | E | R | E | D | S | A | V | E | Y | O | U | R | S | E | L | F |
| Шифрованный текст: | Z | I | C | V | T | W | Q | N | G | R | Z | G | V | T | W | A | V | Z | H | C | Q | Y | G | L | M | G | J |

Расшифровать текст также просто – буква ключа определяет строку, буква шифрованного текста, находящаяся в этой строке, определяет столбец, и в этом столбце в первой строке таблицы будет находиться соответствующая буква открытого текста.

Преимущество этого шифра заключается в том, что для представления одной и той же буквы открытого текста в шифрованном тексте имеется много различных вариантов – по одному на каждую из неповторяющихся букв ключевого слова. Таким образом, скрывается информация, характеризующая частотность употребления букв. Но и с помощью данного метода все же не удается полностью скрыть влияние структуры открытого текста на структуру шифрованного. Повысить надежность шифра поможет использование ключа, длина которого совпадает с длиной сообщения, а текстовые характеристики максимально отклонены от стандартных характеристик языка открытого текста.

Рекомендуемая литература (2, 5, 6)

**Тема 4.** Методы шифрования данных. Метод вертикальной перестановки.

План занятия:

1. Разработать универсальный программный продукт, реализующий шифрование данных, используя метод вертикальной перестановки.

2. Разработать универсальный программный продукт, реализующий дешифрование данных, используя метод вертикальной перестановки.

3. Выполнить индивидуальное задание, согласно своему варианту, и оформить результаты работы в виде отчета.

Контрольные вопросы:

1. Алгоритм шифрования данных.
2. Алгоритм дешифрования данных.
3. Требования к ключу.

Методические рекомендации по выполнению задания:

**Теоретические сведения**

Шифр «Лесенка» особой сложности для криптоанализа не представляет. Более сложная схема предполагает запись текста сообщения в горизонтальные строки одинаковой длины и последующее считывание текста столбец за столбцом, но не по порядку, а в соответствии с некоторой перестановкой столбцов. Порядок считывания столбцов при этом становиться ключом алгоритма. Ниже приведен пример шифрования фразы «ПЕРЕСТАНОВКА ТЕКСТА ПО СТОЛБЦАМ» с ключом 4312567.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Ключ: | 4 | 3 | 1 | 2 | 5 | 6 | 7 |
| Открытый текст: | П | Е | Р | Е | С | Т | А |
| | Н | О | В | К | А | Т | Е |
| | К | С | Т | А | П | О | С |
| | Т | О | Л | Б | Ц | А | М |

Шифрованный текст: РВТЛЕКАБЕОСОПНКТСАПЦТТОААЕСМ

Простой перестановочный шифр очень легко распознать, так как буквы в нем встречаются с той же частотой, что и в открытом тексте. Например, для только что рассмотренного способа шифрования с перестановкой столбцов анализ шифра выполнить достаточно просто – необходимо записать шифрованный текст в виде матрицы и перебрать возможные варианты перестановок для столбцов.

Перестановочный шифр можно сделать существенно более защищенным, выполнив шифрование с использованием перестановок несколько раз. Оказывается, что в этом случае примененную для шифрования перестановку воссоздать уже не так просто. Например, если предыдущее сообщение шифровать еще раз с помощью того же самого алгоритма, то результат будет следующим:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| Ключ: | 4 | 3 | 1 | 2 | 5 | 6 | 7 |
| Открытый текст: | Р | В | Т | Л | Е | К | А |
| | Б | Е | О | С | О | П | Н |
| | К | Т | С | А | П | Ц | Т |
| | Т | О | А | А | Е | С | М |

Шифрованный текст: ТОСАЛСААВЕТОРБКТЕОПЕКПЦСАНТМ

**Варианты индивидуальных заданий**

В ходе анализа ряда перехваченных сообщений, шифруемых методом вертикальной перестановки, криптоаналитиками был частично восстановлен используемый при этом ключ. В частности, они определили количество символов в ключе, а так же числовые значения некоторых позиций. Результат работы криптоаналитиков представлен в виде строки, длина которой совпадает с длиной ключа, а символом X отмечены позиции ключа, значения которых на текущий момент неизвестны (см. задание в таблице). От Вас требуется по имеющемуся шифртексту закончить восстановление ключа и получить открытый текст, соответствующий шифрованному сообщению.

| Вариант | Задание |
|---|---|
| 1. | Зашифрованный текст:<br>ФТБЕОЗРЬЩМАОСЕОИАОИНШВОНЖ<br>Частично восстановленный ключ: XX5X1 |

| | |
|---|---|
| 2. | Зашифрованный текст:<br>ПНОСОЕЕНМРЗОЮЯАЬЬАПТКТБС<br>Частично восстановленный ключ: 6XX1X4 |
| 3. | Зашифрованный текст:<br>ОННАНЦОНДЛЬХФИСНИАТЫКЕЬД<br>Частично восстановленный ключ: XX24X3 |
| 4. | Зашифрованный текст:<br>СИВОСЕНЕЗОПЕОПТОЧЕБСЕСЙАИБЕТЕН<br>Частично восстановленный ключ: 4XX13X |
| 5. | Зашифрованный текст:<br>СНСКЫЕЕОАНОЕЕУАБЧДПНПИТДМ<br>Частично восстановленный ключ: 3XXX5 |
| 6. | Зашифрованный текст:<br>АКДВСЕШНЛСООСИЫАЧЕФЯКЕТРИМИИ<br>Частично восстановленный ключ: 63XX27X |
| 7. | Зашифрованный текст:<br>ИАОТЮОЕРКМФНТЫЧРИКМОШВСЫЛ<br>Частично восстановленный ключ: XX3X2 |
| 8. | Зашифрованный текст:<br>ЛЩЕОЬИЙМААТЛНТОАОЯСВКЗЕЗЛААТ<br>Частично восстановленный ключ: 7XX3X24 |
| 9. | Зашифрованный текст:<br>СУХЫЫМИЗЕМТРОТНАНЦПЙАЗИАЛЕИЩФИЬМЗИОИ<br>Частично восстановленный ключ: 2XX3X6 |
| 10. | Зашифрованный текст:<br>БСЕАГНМЗЛАЕООЯНПЛТБНАЕЕСЬЬЕА<br>Частично восстановленный ключ: 2X41XX7 |

Рекомендуемая литература (2, 5, 6)

**Тема 5.** Методы шифрования данных. Метод Плейфейра.

План занятия:

1. Разработать универсальный программный продукт, реализующий шифрование данных, используя метод Плейфейра.
2. Разработать универсальный программный продукт, реализующий дешифрование данных, используя метод Плейфейра.
3. Выполнить индивидуальное задание, согласно своему варианту, и оформить результаты работы в виде отчета.

Контрольные вопросы:

1. Алгоритм шифрования данных.
2. Алгоритм дешифрования данных.
3. Требования к ключу.

Методические рекомендации по выполнению задания:

**Теоретические сведения**

Одним из наиболее известных шифров, базирующихся на методе многобуквенного шифрования, является шифр Плейфейера (Playfair), в котором биграммы открытого текста рассматриваются как самостоятельные единицы, преобразуемые в заданные биграммы шифрованного текста.

Алгоритм Плейфейера основан на использовании матрицы букв размерности 5×5, созданной на основе некоторого ключевого слова. Матрица создается путем размещения букв, использованных в ключевом слове, слева направо и сверху вниз. Затем оставшиеся буквы алфавита размещаются в естественном порядке в оставшихся строках и столбцах матрицы. Буквы I и J считаются одной и той же буквой. Ниже приведен пример такой матрицы для ключевого слова *monarchy* (монархия).

| M | O | N | A | R |
|---|---|---|---|---|
| C | H | Y | B | D |
| E | F | G | I/J | K |
| L | P | Q | S | T |
| U | V | W | X | Z |

Открытый текст шифруется порциями по две буквы в соответствии со следующими правилами.

1. Если оказывается, что повторяющиеся буквы открытого текста образуют одну пару для шифрования, то между этими буквами вставляется специальная буква-заполнитель, например *X*. В частности, такое слово как *balloon* будет преобразовано к виду ba lx lo on.
2. Если буквы открытого текста попадают в одну и ту же строку матрицы, каждая из них заменяется буквой, следующей за ней в той же строке справа – с тем условием, что для замены последнего элемента строки матрицы служит первый элемент той же строки. Согласно выше построенной матрицы AR шифруется как RM.
3. Если буквы открытого текста попадают в один и тот же столбец матрицы, каждая из них заменяется буквой, состоящей в том же столбце сразу под ней, с тем условием, что для замены самого нижнего элемента столбца матрицы берется самый верхний элемент того же столбца. В примере выше MU шифруется как CM.
4. Если не выполняется ни одно из приведенных условий, каждая буква из пары букв открытого текста заменяется буквой, находящейся на пересечении содержащей эту букву строки матрицы и столбца, в котором находится вторая буква открытого текста. Например, HS шифруется как BP, а EA – как IM (или JM, по желанию шифровальщика).

Шифр Плейфейера значительно надежнее простых моноалфавитных шифров. С одной стороны, букв всего 26, а биграмм - 26×26 = 676, и уже поэтому идентифицировать биграммы сложнее, чем отдельные буквы. С другой стороны, относительная частота появления отдельных букв колеблется гораздо в более широком диапазоне, чем частота появления биграмм, поэтому анализ частотности употребления биграмм тоже оказывается сложнее анализа частотности употребления букв. По этим причинам очень долго считалось, что шифр Плейфейера взломать невозможно. Он служил стандартом шифрования в Британской армии во время первой мировой войны и нередко применялся в армии США и союзных войсках даже в период второй мировой войны.

Несмотря на столь высокую репутацию в прошлом, шифр Плейфейера на самом деле вскрыть относительно легко, так как шифрованный с его помощью текст все равно сохраняет многие статистические характеристики открытого текста. Для взлома этого шифра, как правило, достаточно иметь шифрованный текст, состоящий из нескольких сотен букв.

**Варианты индивидуальных заданий**

При использовании шифра Плейфейера на базе русского языка из алфавита удаляются буквы Ё (заменяется буквой Е) и буква Й (заменяется буквой И). Буквы Ъ и Ь считаются одной и той же буквой. Матрица букв строится на алфавите

АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ,

состоящем из 31 буквы, и состоит из 5 строк и 6 столбцов. Например, матрица букв на базе ключевого слова ПАРУСНИК будет выглядеть следующим образом:

| П | А | Р | У | С | Н |
|---|---|---|---|---|---|
| И | К | Б | В | Г | Д |
| Е | Ж | З | Л | М | О |
| Т | Ф | Х | Ц | Ч | Ш |
| Щ | Ъ/Ь | Ы | Э | Ю | Я |

Возьмите из таблицы ключевое слово и последовательность символов, соответствующие Вашему варианту. Используя ключевое слово и шифр Плейфейера, закодируйте фразу «КОД ПЛЕЙФЕЙЕРА ОСНОВАН НА ИСПОЛЬЗОВАНИИ МАТРИЦЫ БУКВ» и декодируйте указанную в задании последовательность символов.

| Вариант | Задание |
|---|---|
| 1. | Ключевое слово: ПОЛЕТ<br>Строка для декодирования:<br>КЛКЕПЕШОБКЕРЭЛЧСКУЛЮЕТВМВКИММЮЗОТЖША |
| 2. | Ключевое слово: ФИЛЬМ<br>Строка для декодирования:<br>НПВЪЗПЖИКЛБЦРПЪПЭИЯЩЛИЗПБКФАГПШУХЭЧЖРЫВЦТУНЧТЩЧНХНЩТНЯХКДНЦВЗТЧИ |
| 3. | Ключевое слово: КАТЕР<br>Строка для декодирования:<br>ЗЛНЖКГСЩЯЪАОЕСМЩЯСОЛКДБОУЩФРКЖФТАРТЮВИОАСЫЫРМРЕПМЩ |
| 4. | Ключевое слово: ПАРОЛЬ<br>Строка для декодирования:<br>ЮОГНФПЛМКЮМВРМХИНЦШБЛГЖМУПЕАЮЖЧЗПДАМАЛНЪЖЕАДПУНЕЛСЪМЧПМЪЗЧЪЭАЩЩЦНТЗЗУАД |
| 5. | Ключевое слово: КОЛЬЦА<br>Строка для декодирования:<br>МИПГПДПМЖВТЩВИЕИЛРЩЧЗОЛИНЦЩХЖПЪРВЦТУОЖАЫВХУКЖЕВИ |
| 6. | Ключевое слово: КАМЕНЬ<br>Строка для декодирования:<br>РСРФЪПЧСВЛНПНЪСШТОБСХЪИЪФОПГИМФАНЪУКГЩЛНВНКХЧЪДУНЛМАХКСЛИЧТБЕУ |
| 7. | Ключевое слово: СОЛНЦЕ<br>Строка для декодирования:<br>ЗОИЦОЫИТЗУСОШЖАЦФАВЗЗКЗЧНБЗЖУКПБЕЫТЗЪЗФЩ |
| 8. | Ключевое слово: ТОВАРИЩ<br>Строка для декодирования:<br>МОЩЕЯВЧЪЛТАПЯВМОМРЗФИЫПТБКВИХБЦБЩШЪЧШЩИВТЧОАДХОПАБТИВАРМЖИ |
| 9. | Ключевое слово: СВЯЗЬ<br>Строка для декодирования:<br>ЛМЧШЮГХТЯПХООПКПЖМКЧВЦАОБФЖГКХПНЯВЖФЪЛЯНХОФЗТЪСЦПИЛФЛЪ |
| 10. | Ключевое слово: МАТЕРИЯ<br>Строка для декодирования:<br>УЕНАЕЭМЧЗПФТКСЪИАРУЕПЕСЯЕХТИСЩГХМЖФЗЧБГЩКМЮАЕЪ |

Рекомендуемая литература (2, 5, 6)

**Тема 6.** Методы шифрования данных. Метод поворотной решетки.

План занятия:

1. Разработать универсальный программный продукт, реализующий шифрование данных, используя метод поворотной решетки.

2. Разработать универсальный программный продукт, реализующий дешифрование данных, используя метод поворотной решетки.

Контрольные вопросы:

1. Алгоритм шифрования данных.
2. Алгоритм дешифрования данных.
3. Требования к ключу.

Методические рекомендации по выполнению задания:

**Теоретические сведения**

Для использования шифра, называемого поворотной решеткой, изготавливается трафарет из прямоугольного листа клетчатой бумаги размером $2m \times 2n$ клеток. В трафарете вырезано $m \times n$

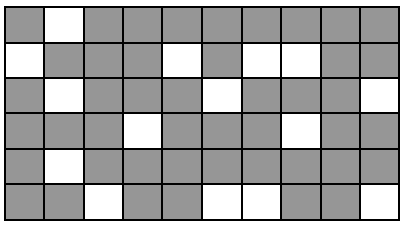
клеток так, что при наложении его на чистый лист бумаги того же размера четырьмя возможными способами его вырезы полностью покрывают всю площадь листа.

Буквы сообщения последовательно вписываются в вырезы трафарета (по строкам, в каждой строке слева направо) при каждом из четырех его возможных положений в заранее установленном порядке.

Рассмотрим процесс шифрования на примере. Пусть в качестве ключа используется решетка 6 × 10, приведенная на рисунке, *а*. Зашифруем с ее помощью текст

ШИФРРЕШЕТКАЯВЛЯЕТСЯЧАСТНЫМСЛУЧАЕМШИФРАМАРШРУТНОЙПЕРЕСТАНОВКИ.

а)



б)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Ш | | | | | | | | |
| И | | | | Ф | | Р | Р | | |
| | Е | | | | Ш | | | | Е |
| | | | Т | | | | К | | |
| | А | | | | | | | | |
| | | Я | | | В | Л | | | Я |

в)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Е | Ш | | Т | С | | | Я | | |
| И | | | | Ф | | Р | Р | Ч | |
| | Е | А | | | Ш | С | | | Е |
| | | | Т | Н | | | К | Ы | |
| | А | М | С | | Л | | | | У |
| | | Я | | | В | Л | | Ч | Я |

г)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Е | Ш | А | Т | С | Е | М | Я | | Ш |
| И | И | | | Ф | | Р | Р | Ч | |
| | Е | А | Ф | | Ш | С | Р | | Е |
| Т | А | | Т | Н | М | | К | Ы | А |
| Р | А | М | С | Ш | Л | Р | У | | У |
| | Т | Я | | | В | Л | | Ч | Я |

д)

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Е | Ш | А | Т | С | Е | М | Я | Н | Ш |
| И | И | О | Й | Ф | П | Р | Р | Ч | Е |
| Р | Е | А | Ф | Е | Ш | С | Р | С | Е |
| Т | А | Т | Т | Н | М | А | К | Ы | А |
| Р | А | М | С | Ш | Л | Р | У | Н | У |
| О | Т | Я | В | К | В | Л | И | Ч | Я |

*Рис.* Пример шифрования текста методом поворотной решетки.

Наложив решетку на лист бумаги, вписывается первые 15 (по числу вырезов) букв сообщения. Результат после снятия решетки изображен на рисунке, *б*. Повернув решетку на 180 градусов и вписав следующие 15 букв, получаем лист, изображенный на рисунке 3, *в*. Перевернув лист и проделав то же самое, шифруется остаток текста (рисунок, *г* и *д*).

Получатель сообщения, имеющий точно такую же решетку, без труда прочтет исходный текст, наложив решетку на шифртекст по порядку четырьмя способами.

Число трафаретов, то есть количество ключей шифра «решетка», составляет $T = 4^{mk}$. Этот шифр предназначен для сообщений длины $n = 4mk$. Уже при размере трафарета 8 × 8 число возможных решеток превосходит 4 миллиарда.

Рекомендуемая литература (2, 5, 6)

## 8. Задания для самостоятельной работы

**Тема 1 -** Введение. Защита информации

Цель: Изучить виды безопасности, методы противодействия информационным угрозам, получить представление о роли и месте системы обеспечения информационной безопасности для государства в целом.

Содержание: Понятие национальной безопасности. Виды безопасности: государственная, экономическая, общественная, военная, экологическая, информационная. Информационные

угрозы. Противодействие информационным угрозам. Роль и место системы защиты и безопасности информации в современном информационном процессе

**Тема 2 –** Безопасность информации.

Цель: Получить представление о системах защиты информации, изучить их особенности и основные характеристики.

Содержание: Системы защиты информации. Особенности и основные характеристики. Методы обеспечения безопасности информации. Средства обеспечения безопасности информации.

**Тема 4 –** Модели безопасности информационных систем.

Цель: Изучить основные модели безопасности, политику безопасности, а также виды стандартов в области информационной защиты и безопасности и их структуру.

Содержание: Формальные модели. Модели безопасности. Политика безопасности. Критерии и классы защищенности средств вычислительной техники и автоматизированных информационных систем. Стандарты по оценке защищенных систем. Структура стандартов в области информационной защиты и безопасности Республики Казахстан

**Тема 9 –** Оптимальное управление процессами защиты.

Цель: изучить методы оптимального управления процессами обеспечения безопасности на законодательном уровне.

Содержание: Законодательные и нормативные акты Республики Казахстан в области защиты и безопасности информации

## 9. График консультации СРОП (СРОП составляет 25% из СРО)

Консультация по всем вопросам осуществляется согласно графику СРОП на текущий семестр

## 10. Расписание проверок знаний обучающихся

Посещение практических занятий оценивается 0-100 баллов

**График выполнения и сдачи заданий по дисциплине**

| № | Виды работ | Тема, цель и содержание задания | Рекомендуемая литература | Продолжительность выполнения | Форма контроля | Срок сдачи |
|---|---|---|---|---|---|---|
| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| 1 | Практическая работа 1 | Профессиональная деятельность и коммуникация программиста. Сферы профессиональной деятельности: учебная, научная, техническая, производственная. | 1-6 | 1 неделя | конспект | 1-ая неделя |
| 2 | Практическая работа 2 | Профессионализмы, профессиональная речь (специалистов в области программирования). Социальный статус собеседников (руководитель – подчиненный, начальник отдела ИТ – программист; равноправные по статусу – программисты), социальные роли | 1-6 | 1 неделя | конспект | 2-я неделя |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | коммуникантов (инженер-программист, IT-специалист, web-дизайнер и т.д.). | | | | |
| 3 | Практическая работа 3 | Научная речь как составляющая профессиональной культуры программиста. Работа с текстами по специальности: комментированное чтение, терминологический комментарий текста, стилистический анализ текста, комплексный анализ текста, орфографический и пунктуационный анализ текста, составление реферата, критический анализ текста научного стиля и др. | 1-6 | 2 недели | конспект | 4-я неделя |
| 4 | Практическая работа 4 | Прагматические единицы языкового уровня – слово, язык, предложение, текст. Слова с эмоционально-экспрессивной и стилистической окраской. Тексты научного, официально-делового, публицистического стилей. Стили общения – официальный, полуофициальный, неофициальный. Коммуникативные ситуации (в рамках специальности). | 1-6 | 2 недели | конспект | 6-я неделя |
| 5 | Практическая работа 5 | Терминологический минимум в рамках речевой темы «Профессия программиста». Компьютер. Понятие программирования. Языки программирования. Понятие вычислительной техники. Защита информации. Технологии будущего. | 1-6 | 1 неделя | конспект | 7-я неделя |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | Терминологический минимум в рамках речевой темы «Основы вычислительной техники и программирования». | | | | |
| 6 | Рубежный контроль | Защита практических работ | | | конспект, тестирование | 8-ая неделя |
| 7 | Практическая работа 6 | Минимум микротем в рамках темы «Из истории создания вычислительной техники. Абак, логарифмическая линейка, счетный механизм, арифмометр, первый компьютер, архитектура фон Неймана». | 1-6 | 1 неделя | конспект | 9-я неделя |
| 8 | Практическая работа 7 | Минимум микротем в рамках темы «Из истории создания вычислительной техники. Абак, логарифмическая линейка, счетный механизм, арифмометр, первый компьютер, архитектура фон Неймана». | 1-6 | 1 неделя | конспект | 10-я неделя |
| 9 | Практическая работа 8 | Типы служебных документов – внутренние и внешние; распорядительные, отчетные, плановые; научные, технические, юридические, производственные, финансовые. Постановление. Решение. Приказ. Распоряжение. Указание. Акт. Справка. Заявление. | 1-6 | 1 неделя | конспект | 11-я неделя |
| 10 | Практическая работа 9 | Официальные письма – деловая и | 1-6 | 1 неделя | конспект | 12-я неделя |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | коммерческая корреспонденция. Основные виды коммерческой корреспонденции – коммерческий запрос, ответ на запрос, письмо-предложение (оферта), ответ на предложение, письмо-претензия (рекламация), ответ на рекламацию, информационно-рекламные письма. Язык и стиль документов – языковые формулы, речевой этикет в документе. | | | | |
| 11 | Практическая работа 10 | Юридические и правовые документы. Финансовые документы. Контракт, договор, меморандум, соглашение. Презентация. Резюме. Реклама. Рекомендательное письмо. | 1-6 | 1 неделя | конспект | 13-я неделя |
| 12 | Практическая работа 11 | Научные и специальные технологии. Информационно-коммуникационные технологии, IT-технологии, Интернет-технологии. | 1-6 | 1 неделя | конспект | 14-я неделя |
| 13 | Практическая работа 12 | Особенности речи специалиста. Культура речи специалиста. Способность к абстрагированию и пониманию отношений между элементами, гибкость мышления, критичность, склонность к планированию, анализу и систематической работе, готовность пополнять знания и переучиваться. | 1-6 | 1 неделя | конспект | 15-я неделя |
| 14 | Рубежный | Защита практических | | | конспект, | 15-ая |

| | | | | | | |
|---|---|---|---|---|---|---|
| | контроль | работ | | | тестирование | неделя |

## 11. Критерии оценки знаний обучающихся

Изучение дисциплины заканчивается экзаменом в форме тестирования, который охватывает весь пройденный материал. Обязательным условием для допуска к экзамену является выполнение всех предусмотренных заданий в программе.

Каждое задание оценивается 0-100 баллов.

Рейтинг допуска выводится из средне арифметического всех выполненных заданий на текущих занятиях (посещение лекции, домашние задания, задания по СРО, задания по практике и другие, рубежный контроль).

К итоговому контролю (ИК) по дисциплине допускаются студенты, выполнившие все требования рабочей учебной программы (выполнение и сдача всех лабораторных работ, работ и заданий по СРС), получившие положительную оценку за защиту курсового проекта (работы) и набравшие рейтинг допуска (не менее 50 баллов).

Уровень учебных достижений студентов по каждой дисциплине (в том числе и по дисциплинам, по которым формой итогового контроля ГЭ) определяется итоговой оценкой (И), которая складывается из оценок РД и ИК (экзамена, дифференцированного зачета или курсовой работы/проекта) с учетом их весовых долей (ВДРД и ВДИК).

И = РД*0,6 + ИК*0,4

Весовые доли ежегодно утверждаются ученым советом университета и должны быть для РД не более 0,6, а для ИК не менее 0,3.

КП/КР защищаются перед комиссией. Оценка выставляется в соответствии с продемонстрированными знаниями с учётом отзыва руководителя.

Итоговая оценка по дисциплине подсчитывается только в том случае, если обучающийся имеет положительные оценки, как по рейтингу допуска, так и по итоговому контролю. Не явка на итоговый контроль по неуважительной причине приравнивается к оценке «не удовлетворительно». Результаты экзамена и промежуточной аттестации по дисциплине доводятся до студентов в тот же день или на следующий день, если письменный экзамен проводился во второй половине дня.

Для корректности подсчета итоговой оценки знания обучающегося на рубежном контроле (рейтинге) и итоговом экзамене оцениваются в процентах от 0 до 100%.

Оценка рубежного контроля складывается из текущих оценок и оценки рубежного контроля.

Учебные достижения, то есть Знания, умения, навыки и компетенции студентов по дисциплине «Финансы» оцениваются по многобалльной буквенной системе адекватной ее цифровому эквиваленту и традиционной шкале оценок:

| Оценка по буквенной системе | Цифровой эквивалент баллов | Процентное содержание | Оценка по традиционной системе |
|---|---|---|---|
| A | 4,0 | 95-100 | Отлично |
| A- | 3,67 | 90-94 | |
| B+ | 3,33 | 85-89 | Хорошо |
| B | 3,0 | 80-84 | |
| B- | 2,67 | 75-79 | |
| C+ | 2,33 | 70-74 | Удовлетворительно |
| C | 2,0 | 65-69 | |
| C- | 1,67 | 60-64 | |
| D+ | 1,33 | 55-59 | |
| D | 1,0 | 50-54 | |
| F | 0 | 0-49 | Неудовлетворительно |

## 12. Требования преподавателя, политика и процедуры

Посещение обучающимися всех аудиторных занятий без опозданий является обязательным. В случае пропуска занятия отрабатываются в порядке установленном деканатом. Допускается максимально только два пропуска занятий. Два опоздания на занятие приравниваются одному пропуску. В случае более двух пропусков преподаватель имеет право в дальнейшем студента не допускать к занятиям до административного решения вопроса. Присутствие на лекциях посторонних лиц, не являющихся контингентом студентов данного курса, запрещается.

Работы следует сдавать в указанные сроки. Крайний срок сдачи всех заданий – за 3 дня до начала экзаменационной сессии.

Студенты, не сдавшие все задания, и не защитившие курсовую работу, не допускаются к экзамену.

Повторение темы и отработка пройденных материалов по каждому учебному занятию обязательны. Степень освоения учебных материалов проверяется тестами или письменными работами. Тестирование студентов может проводиться без предупреждения.

**При выполнении самостоятельной работы студентов под руководством преподавателя (СРСП) учитывать следующие четыре основные функции.**

Первая – предполагает реализацию активного восприятия студентами информации преподавателя, полученной в период установочных занятий по учебной дисциплине.

Вторая функция предполагает, что студенты самостоятельно, на основании рекомендаций преподавателя, изучают учебно-методические пособия, литературные источники, выполняют домашние задания, контрольные и курсовые работы и т.д. На этом этапе от студентов требуется знание методов работы, фиксация своих затруднений, самоорганизация и самодисциплина.

Третья функция студентов состоит в анализе и систематизации своих затруднительных ситуаций, выявлении причин затруднений в понимании и усвоении ими учебного материала, выполнении других учебных действий. Студенты переводят неразрешимые затруднения в систему вопросов для преподавателя (ранжируют их, упорядочивают, оформляют), строят собственные версии ответов на эти вопросы.

Четвертая функция студентов состоит в обращении к преподавателю за соответствующими разъяснениями, советами, консультациями.

## 13. Список литературы


Основная:

1) Завгородний В.И. Комплексная защита информации в компьютерных системах: Учебное пособие. – М.: Логос; ПБОЮЛ Н.А. Егоров, 2001.

2) Скляров Д.В. Искусство защиты и взлома информации. — СПб.: БХВ-Петербург, 2004.

3) Жельников В. Криптография от папируса до компьютера. – М.: Dore Print, 1999.

4) Сёмкин С.Н., Беляков Э.В., Гребенёв С.В., Козачёк В.И. Основы организационного обеспечения информационной безопасности объектов информатизации. – М.: «Гелиос АРВ», 2005.

5) Саломаа А. Криптография с открытым ключом: Пер. с англ. — М.: Мир, 1995.

6) Хорошко В.А.. Чекатков. Методы и средства защиты информации. — Вінниця: ВДТУ, 2003.

Дополнительная:

7) Законодательные акты РК в области защиты и безопасности информации.

8) Нормативные документы РК в области защиты и безопасности информации.

9) Грушко А.А., Тимонина Е.Е. Теоретические основы защиты информации.-М.: «Яхстмен»,1996.

10) Хореев А.А. Способы и средства защиты информации. Учебное пособие.-М.: МО РФ, 2000.


## 14. Список мультимедийного сопровождения

1) Fine Reader 5.0

2) MS Office

3) Borland Delphi 7.0