Государственное образовательное учреждение
«Приднестровский государственный университет им. Т.Г. Шевченко»
Рыбницкий филиал

Кафедра информатики и программной инженерии

УТВЕРЖДАЮ
Зав. кафедрой
_____ Тягульская Л.А., доцент
Протокол № 2 от «23» 09 2021 г.

Фонд оценочных средств

по дисциплине

«СЕТЕВЫЕ ТЕХНОЛОГИИ»

Направление подготовки:
2.09.03.04 «Программная инженерия»

Профиль подготовки:
«Разработка программно-информационных систем»

Квалификация
Бакалавр

Форма обучения
очная заочная

2018 год набора

Разработал:
ст. преподаватель _____ А.Б. Глазов
«24» сентября 2021 г.

Паспорт фонда оценочных средств по учебной дисциплине

1. В результате изучения дисциплины «Сетевые технологии» у обучающихся должна быть сформирована следующая компетенция:

Код компетенции	Формулировка компетенции
ПК-2	Владением навыками использования операционных систем, сетевых технологий, средств разработки программного интерфейса, применения языков и методов формальных спецификаций, систем управления базами данных

В результате освоения дисциплины студент должен:

3.1. Знать:

– принципы функционирования вычислительных сетей и комплексов;

– основные решения по построению физического, канального, сетевого и транспортного уровней;

– методы и способы программной реализации сетевого взаимодействия в вычислительных сетях.

3.2. Уметь:

– на основе полученных знаний формулировать и решать задачи проектирования и модернизации локальной или корпоративной вычислительной сети, а также глобальной сети;

– конфигурировать сетевые устройства;

– оценивать трафик в сегментах сети;

– выбирать состав сетевого оборудования и программного обеспечения.

3.3. Владеть навыками:

– продемонстрировать соединения компонентов сетевого оборудования в единый комплекс;

– использования предоставляемого операционной системой пользовательского интерфейса конфигурирования сетевой операционной среды.

2. Программа оценивания контролируемой компетенции:

Текущая аттестация	Контролируемые модули, разделы (темы) дисциплины и их наименование	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1	Основные понятия и определения	ПК-2	– **текущий** – контроль выполнения лабораторных работ, тестирование; – **рубежный** предполагает использование тестовых материалов для контроля знаний.
2	История развития криптографии как науки	ПК-2	
3	Современные криптографические системы	ПК-2	
4	Защита программного обеспечения	ПК-2	
5	Сетевые технологии в рамках организации	ПК-2	
6	Сетевые технологии на государственном уровне	ПК-2	
Промежуточная аттестация		**Код контролируемой компетенции (или ее части)**	**Наименование оценочного средства**
1		ОПК-1, ОПК-2, ПК-1	Тест. Курсовая работа. Вопросы к экзамену

УТВЕРЖДАЮ
зав. кафедрой информатики и программной инженерии,
доцент_____ Л.А. Тягульская
«___»_____2021 г.

Темы курсовых работ
по дисциплине «Сетевые технологии»
для студентов IV курса
направления «Программная инженерия»
профиля «Разработка программно-информационных систем»,
7 семестр

1. Сетевая игра в домино «Козел».
2. Сетевая игра в домино «Пятерка».
3. Сетевая игра в карты «Дурак».
4. Сетевая игра в карты «Blackjack».
5. Сетевая игра в кости.
6. Динамический анализ курсов валют.
7. Анализ изменения температуры по годам и регионам.
8. Анализ изменения влажности по годам и регионам.
9. Онлайн-анкетирование социальной тематике.
10. Простой голосовой чат.
11. Сетевой чат на Web Sockets.
12. Сайт для портфолио студента.
13. Удаленное управление компьютером.
14. SPA сайт с переменными темами оформления.
15. Простой аналог PHP Admin.
16. Сетевая игра в крестики-нолики.
17. Сайт по интерактивному обучению Pascal.
18. Реализация игры «Арканоид».
19. Разработка игры с сетевыми элементами.
20. Разработка сайта с использованием DBSN.
21. Сайт для организации работы поисковых систем.
22. Программа тестирование сервиса адаптации HTML-тегов для WordPress.

Составитель _____ А.Б. Глазов, ст. преподаватель

УТВЕРЖДАЮ
зав. кафедрой информатики и программной инженерии,
доцент_____ Л.А. Тягульская
«___»_____2021 г.

Вопросы к экзамену
по дисциплине «Сетевые технологии»
для студентов IV курса
направления «Программная инженерия»
профиля «Разработка программно-информационных систем»,
7 семестр - 02
8 семестр - 30

1. Терминология и принципы организации сетей, основные понятия.
2. Основы работы Internet.
3. Стек протоколов OSI – общий обзор.
4. Стек протоколов TCP/IP начало.
5. Классификация сетей по размеру и по топологии, кольцо шина маркерный доступ.
6. Способы кодирования сигналов на физическом уровне.
7. Протокол Ethernet.
8. Сетевое оборудование.
9. Протокол ARP.
10. Прохождение IP пакета между сетями.
11. Классовая адресация IP сетей.
12. Бесклассовая адресация IP сетей.
13. Разбиение пула IP адресов на подсети.
14. Протокол UDP.
15. Протокол DHCP.
16. Протокол TFTP
17. Протокол TCP.
18. Протокол Telnet.
19. FTP клиент-сервер.
20. DNS сервера и система имен.
21. Введение в Python 3, установка.
22. Python функции.
23. Python: работа с массивами, число слов в тексте, список разных слов в тексте.
24. Python – средства работы с диском.
25. Сокеты на Python.
26. Запуск из Python внешнего приложения.
27. Python Генераторы Списков.
28. Python – основы работы в сети.
29. Применение Python для сетевых игр.
30. Python tcpserver.py, tcpclient.py.
31. Python udpserver.py, udpclient.py.
32. Чат на основе UDP протокола.
33. Python ftpclient, ftpserver.
34. Команда консольного режима Net.
35. Расчет оборудования компьютерной сети.
36. Запуск из Python внешнего приложения.
37. Python – основы работы в сети.
38. Запуск из Python внешнего приложения.
39. Python – основы работы в сети.
40. Способы передачи пакетов.

41. Запуск из Python внешнего приложения.
42. Python – основы работы в сети.
43. Программы TeamViewer, A3, Radmin.
44. Настройка сетевого подключения.
45. Консольные средства диагностики.
46. Методы управления трафиком.
47. Администрирование компьютерных сетей.
48. Практика по сниферам WireShark, ComView.
49. Обжимка кабеля сдача практики по расчету материалов для локальной сети.
50. Работа с Ethernet на канальном уровне. Простой снифер на Python.
51. Элементы протокола IP, IP adresa.
52. Элементы парсинга сайтов с Beautifulsoup.
53. Обзор Teamviewer, ICQ. Первичная настройка сети.
54. Утилиты консольной диагностики сети.

Составитель _____ А.Б. Глазов, ст. преподаватель

УТВЕРЖДАЮ
зав. кафедрой информатики и программной инженерии,
доцент_____ Л.А. Тягульская
«___»_____2021 г.

Примеры индивидуальных заданий
по дисциплине «Сетевые технологии»
для студентов IV курса
направления «Программная инженерия»
профиля «Разработка программно-информационных систем»,
7 семестр

Программа самостоятельной работы по дисциплине «Сетевые технологии» предполагает выполнение студентом в процессе обучения одного индивидуального задания из следующего списка индивидуальных заданий по компьютерным алгоритмам СЗИ:

1. Стандарт симметричного шифрования данных DES.
2. Блочный шифр IDEA.
3. Блочный шифр ГОСТ.
4. Блочный шифр CAST.
5. Блочный шифр BLOWFISH.
6. Блочный шифр RC5.
7. Блочный шифр LUCIFER.
8. Блочный шифр MADRYGA.
9. Блочный шифр NewDES.
10. Блочный шифр FEAL.
11. Блочный шифр REDOC.
12. Блочный шифр LOKI.
13. Блочный шифр KHUFU.
14. Блочный шифр RC2.
15. Блочный шифр MMB.
16. Блочный шифр CA-1.1.
17. Блочный шифр SKIPJACK.
18. Блочный шифр SAFER.
19. Блочный шифр 3-WAY.
20. Блочный шифр CRAB.
21. Блочный шифр SXAL8/MBAL.
22. Блочный шифр RC4.
23. Блочный шифр SEAL.
24. Асимметричный ранцевый криптоалгоритм.
25. Асимметричный алгоритм шифрования данных RSA.
26. Асимметричный алгоритм шифрования данных ElGamal.
27. Асимметричный алгоритм шифрования данных Pohlig-Hellman.
28. Асимметричный алгоритм шифрования данных Rabin.
29. Асимметричный алгоритм шифрования данных McEliece
30. Асимметричный алгоритм шифрования данных LUC.
31. Алгоритм цифровой подписи с открытым ключом DSA.
32. Алгоритм цифровой подписи с открытым ключом ГОСТ.
33. Однонаправленная хэш-функция Snefru.
34. Однонаправленная хэш-функция *N*-хэш.
35. Однонаправленная хэш-функция MD4.
36. Однонаправленная хэш-функция MD5.
37. Алгоритм безопасного хэширования (Secure Hash Algorithm, SHA).
38. Однонаправленная хэш-функция RIPE-MD.
39. Однонаправленная хэш-функция HAVAL.

УТВЕРЖДАЮ
зав. кафедрой информатики и программной инженерии,
доцент_____ Л.А. Тягульская
«___»_____2021 г.

Образец теста
для среза текущих знаний

Указания: *Напишите Вашу фамилию, номер группы и дату. Для ответа на вопрос с выбором варианта ответа достаточно написать номер вопроса и рядом букву, обозначающую правильный вариант из предложенных в тексте ответов на вопрос. Если Вы считаете правильными несколько вариантов ответов, то запишите через запятую соответствующие литеры букв.*

1) Под угрозой безопасности информации в компьютерной системе (КС) понимают:
a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.
c) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

2) Уязвимость информации — это:
a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.
c) это действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

3) Атакой на КС называют:
a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.
b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.
c) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

4) Искусственные угрозы исходя из их мотивов разделяются на:
a) непреднамеренные и преднамеренные
b) косвенные и непосредственные
c) несанкционированные и сонкцианированные

5) К непреднамеренным угрозам относятся:
a) ошибки в разработке программных средств КС
b) несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями.
c) угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой;

6) К умышленным угрозам относятся:
a) несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС);
b) воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.
c) ошибки пользователей КС;

7) Косвенными каналами утечки называют:
a) каналы, не связанные с физическим доступом к элементам КС
b) каналы, связанные с физическим доступом к элементам КС

c) каналы, связанные с изменение элементов КС и ее структуры.

8)К косвенным каналам утечки информации относятся:

a) использование подслушивающих (радиозакладных) устройств;

b) маскировка под других пользователей путем похищения их идентифицирующей информации (паролей, карт и т.п.);

c) злоумышленное изменение программ для выполнения ими несанкционированного копирования информации при ее обработке;

9)Непосредственными каналами утечки называют:

a) каналы, связанные с физическим доступом к элементам КС.

b) каналы, не связанные с физическим доступом к элементам КС

c) каналы, связанные с изменение элементов КС и ее структуры.

10)К непосредственным каналам утески информации относятся:

a) обход средств разграничения доступа к информационным вследствие недостатков в их программном обеспечении и др.

b) перехват побочных электромагнитных излучений и (ПЭМИН).

c) дистанционное видеонаблюдение;

11) Избирательная политика безопасности подразумевает, что:

a) права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

b) все субъекты и объекты системы должны быть однозначно идентифицированы;

c) каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации;

12) Полномочная политика безопасности подразумевает, что:

a) каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ.

b) все субъекты и объекты системы должны быть идентифицированы;

c) права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

13) Уязвимость информации — это:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации.

b) набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа.

c) неизменность информации в условиях ее случайного и (или) преднамеренного искажения или разрушения.

14) Под защитой информации понимается

a) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по проверке целостности информации и исключении несанкционированного доступа к ресурсам ПЭВМ и хранящимся в ней программам и данным.

b) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по реализации механизма виртуальной памяти с разделением адресных пространств;

c) совокупность мероприятий, методов и средств, обеспечивающих решение следующих задач по разграничению прав пользователей и обслуживающего персонала.

15) Возможные каналы утечки информации по классификации разделяют:

a) человек, аппаратура, программа

b) человек, линия связи

c) коммутационное оборудование, человек

16)К группе каналов утечки информации в которой основным средством является человек, относятся следующие утечки:

a) расшифровка программой зашифрованной информации;

b) несанкционированный доступ программы к информации;

c) копирование программой информации с носителей.

17) К группе каналов утечки информации, в которой основным средством является аппаратура, относятся следующие утечки:

a) подключение к ПЭВМ специально разработанных аппаратных средств, обеспечивающих доступ к информации;
b) хищение носителей информации (магнитных дисков, дискет, лент)
c) копирование программой информации с носителей

18) К группе каналов утечки информации в которой основным средством является <u>программа,</u> относятся следующие утечки:

a) несанкционированный доступ программы к информации
b) хищение носителей информации (магнитных дисков, дискет, лент)
c) использование специальных технических средств для перехвата электромагнитных излучений технических средств ПЭВМ.

19) Идентификация объекта – это:

a) одна из функций подсистемы защиты.
b) взаимное установление подлинности объектов, связывающихся между собой по линиям связи.
c) сфера действий пользователя и доступные ему ресурсы КС

20) Процедуру установки сфер действия пользователя и доступные ему ресурсы КС называют:

a) авторизацией
b) аутентификацией
c) Идентификация

21) Авторизация – это:

a) предоставление полномочий
b) подтверждение подлинности
c) цифровая подпись

22) Аутентификация – это:

a) подтверждение подлинности
b) предоставление полномочий
c) цифровая подпись

23) Под компьютерным вирусом понимается:

a) автономно функционирующая программа, обладающая способностью к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ЭВМ.
b) программа имеющая доступ к файлам системы, и имеющая возможность работать с процессами системы.
c) программа не имеющая доступ к файлам системы, и не имеющая возможность работать с процессами системы.

24) Трянские программы это:

a) программы, которые содержат скрытые последовательности команд (модули), выполняющие действия, наносящие вред пользователям.
b) программы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.
c) программы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам.

ОТВЕТЫ

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

УТВЕРЖДАЮ
зав. кафедрой информатики и программной инженерии,
доцент_____ Л.А. Тягульская
«___»_____2021 г.

Образец теста
для проведения итогового контроля по итогам освоения дисциплины, а также для контроля самостоятельной работы студента

Указания: *Напишите Вашу фамилию, номер группы и дату. Для ответа на вопрос с выбором варианта ответа достаточно написать номер вопроса и рядом букву, обозначающую правильный вариант из предложенных в тексте ответов на вопрос. Если Вы считаете правильными несколько вариантов ответов, то запишите через запятую соответствующие литеры букв.*

1) К средствам активной защиты относятся:
a) искаженные программы (программы вирусы, искажение функций)
b) заказное проектирование
c) специальная аппаратура

2) К средствам пассивной защиты относятся:
a) частотный анализ
b) авторская эстетика
c) аппаратура защиты (ПЗУ, преобразователи)

3) К средствам собственной защиты относятся:
a) машинный код
b) сигнатура
c) корреляционный анализ

4) Под системой защиты от несанкционированного использования и копирования понимается:
a) комплекс программных или программно-аппаратных средств, предназначенных для усложнения или запрещения нелегального распространения, использования и (или) изменения программных продуктов и иных информационных ресурсов.
b) комплекс аппаратных и программных средств, предназначенных для автоматизированного сбора, хранения, обработки, передачи и получения информации.
c) комплекс правовых норм, организационных мер, технических, программных и криптографических средств, обеспечивающий защищенность информации в КС в соответствии с принятой политикой безопасности.

5) Под надежностью системы защиты от несанкционированного копирования понимается:
a) способность противостоять попыткам изучения алгоритма ее работы и обхода реализованных в нем методов защиты.
b) способность систем с открытыми ключами генерировать цифровые подписи, обеспечивающие различные функции защиты, компенсирует избыточность требуемых вычислений.
c) способность к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ЭВМ

6) Методы, затрудняющие считывание скопированной информации основываются на
a) придании особенностей процессу записи информации, которые не позволяют считывать полученную копию на других накопителях, не входящих в защищаемую КС
b) разграничении прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц
c) использования дополнительных программных или аппаратно-программных средств.

7) Для защиты от несанкционированного использования программ могут применяться электронные ключи?
a) да

b) нет
c) не знаю

8) Любая криптографическая система основана на использовании:

a) криптографических ключей
b) разомкнутых линии
c) односторонних функций

9) В симметричной криптосистеме отправитель и получатель сообщения используют

a) один и тот же секретный ключ
b) разные секретных ключи
c) вообще не используют секретных ключей

10) Асимметричная криптосистема предполагает использование

a) двух ключей открытого и личного (секретного)
b) системы разграничения доступа
c) переносных носителей для хранения секретной информации

11) Под ключевой информацией понимают:

a) совокупность всех действующих в АСОИ ключей
b) совокупность документов и массивов документов и информационных технологий, реализующих информационные процессы.
c) совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности ее пользователей в соответствии с назначением информации.

12)Какая из функций не входит в процесс управления ключами?

a) переадресация ключей
b) генерация ключей
c) распределение ключей

13) Модификация ключа – это

a) генерирование нового ключа из предыдущего значения ключа с помощью односторонней (однонаправленной) функции.
b) генерирование нового ключа из последующего значения ключа с помощью односторонней (однонаправленной) функции.
c) генерирование нового ключа из предыдущего значения ключа с помощью двусторонней (двунаправленной) функции.

14) Под функцией хранения ключей понимают

a) организацию их безопасного хранения, учета и удаления.
b) организацию их генерации, учета и удаления.
c) организацию их безопасного хранения, учета и сопоставления.

15)В чем заключается правило разграничения доступа

a) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.
b) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа.
c) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, не содержатся все категории, определенные для данного документа.

16) Файловые вирусы это:

a) вирусы, заражающие файлы с программами
b) вирусы, заражающие программы, хранящиеся в системных областях дисков.
c) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам.

17) Резидентные вирусы это:

a) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;
b) вирусы, которые выполняются только в момент запуска зараженной программы.

c) вирусы, заражающие программы, хранящиеся в системных областях дисков.

18) Транзитные вирусы это:

a) вирусы, которые выполняются только в момент запуска зараженной программы.

b) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;

c) вирусы, заражающие программы, хранящиеся в системных областях дисков.

19) Вирусы-мутанты (MtE-вирусы) это

a) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.

b) вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных;

c) вирусы, заражающие программы, хранящиеся в системных областях дисков.

20) Stealth-вирусы это

a) вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных:

b) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.

c) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам.

21) Загрузочные (бутовые) вирусы это:

a) вирусы, заражающие программы, хранящиеся в системных областях дисков.

b) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам.

c) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса.

22) Основной проблемой создания высокоэффективной защиты от НСД является

a) предотвращение несанкционированного перехода пользовательских процессов в привилегированное состояние.

b) использование дополнительных программных или аппаратно-программных средств.

c) разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц

23)Аппаратно-программмные средства криптографической защиты информации выполняют функции:

a) аутентификацию пользователя, разграничение доступа к информации, обеспечение целостности информации и ее защиты от уничтожения, шифрование и электронную цифровую подпись.

b) организовывают реализацию политики безопасности информации на этапе эксплуатации КС.

c) проверяют на отсутствие закладок приборов, устройств.

24) Использование аппаратных средств снимает проблему:

a) обеспечения целостности системы.

b) разграничения прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц

c) использования строго определенного множества программ.

a) за один цикл, и тем самым уменьшает длительность процесса идентификации.

b) внешней аутентификацией объекта, не принадлежащего системе.

ОТВЕТЫ

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