Государственное образовательное учреждение
«ПРИДНЕСТРОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени Т.Г. Шевченко»
Рыбницкий филиал

Кафедра информатики и программной инженерии

«УТВЕРЖДАЮ»
зав. кафедрой ИиПИ,
доцент _____ Л.А. Тягульская
Протокол № _2__
«_21_» *сентября* *2023* г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО ДИСЦИПЛИНЕ
«ЗАЩИТА ИНФОРМАЦИИ»
наименование дисциплины

Направление подготовки:
2.09.03.04 **«Программная инженерия»**
Код наименование направления

Профиль подготовки:
«Разработка программно-информационных систем»
наименование профиля подготовки

Квалификация:
Бакалавр

Форма обучения:
очная

Год набора:
2020

Разработал:
доцент_____Козак Л.Я.
(должность, подпись, ФИО)

Рыбница, 2023 г.

ПАСПОРТ

фонда оценочных средств по учебной дисциплине

1. В результате изучения дисциплины «Защита информации» (Б1.В.12) у обучающихся должны быть сформированы следующие компетенции:

Категория (группа) компетенций	Код и наименование	Код и наименование индикатора достижения компетенции
Общепрофессиональные компетенции и индикаторы их достижения		
Разработка и проектирование	**ОПК-3.** Способен анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров с обоснованными выводами и рекомендациями	ИД-1$_{ОПК-3.1.}$ Знать принципы, методы и средства анализа и структурирования профессиональной информации; ИД-2$_{ОПК-3.2.}$ Уметь анализировать профессиональную информацию, выделять в ней главное, структурировать, оформлять и представлять в виде аналитических обзоров; ИД-3$_{ОПК-3.3.}$ Иметь навыки подготовки научных докладов, публикаций и аналитических обзоров с обоснованными выводами.

2. Программа оценивания контролируемой компетенции:

Текущая аттестация	Контролируемые модули, разделы (темы) дисциплины и их наименование	Код контрол. компетенции (или ее части)	Наименование оценочного средства
1	Раздел 1. Основы информационной безопасности Основные понятия и определения. Политика государства в области информационной безопасности. Угрозы и нарушители безопасности информации	ОПК-3	Комплект тестов Комплект инд. заданий
	Раздел 2. Исторический обзор криптографических методов защиты информации. Меры обеспечения защиты информации	ОПК-3	Темы рефератов
	Раздел 3. Криптографические методы защиты информации. Стенографическая защита информации	ОПК-3	Темы рефератов
2	Раздел 4. Модель угроз безопасности информации. Методы контроля разграничения доступа. Организационные меры защиты информации	ОПК-3	Комплект тестов Комплект инд. заданий
	Раздел 5. Техническая защита информации. Программно-технические методы защиты информации	ОПК-3	Темы рефератов
	Раздел 6. Политика безопасности. Системы обнаружения и предотвращения компьютерных атак	ОПК-3	Темы рефератов
Промежуточная аттестация		**Код контрол. компетенции (или ее части)**	**Наименование оценочного средства**
1		ОПК-3	Комплект КИМ Вопросы к зачету

«УТВЕРЖДАЮ»
зав. кафедрой ИиПИ,
доцент _____ Л.А. Тягульская
«_21__» *сентября* *2023* г.

Вопросы к зачету по дисциплине «Защита информации»
для студентов IV курса направления «Программная инженерия»
профиля подготовки «Разработка программно-информационных систем»,
VII семестр (д/о)

1. Альтернативные методы защиты. Аутентификация по биометрическим данным (отпечаток пальца, геометрия руки, радужная оболочка глаза, сетчатка глаза, голосовая идентификация, геометрия лица, клавиатурный почерк)
2. Асимметричные криптосистемы (алгоритм RSA). Цифровая подпись. Пространство ключей.
3. Базовые направления криптографии: шифрование, кодирование и стеганография. Основные различия.
4. Вредоносное программное обеспечение как средство преодоления защиты информации.
5. Древние методы шифрования: методы перестановок; двойных перестановок. Шифр перестановок магическим квадратом.
6. Древние методы шифрования: шифры алфавитной замены; простой замены; сложной замены.
7. Другие криптографические алгоритмы. Вычисление контрольных сумм (CRC) и хеширование (MD4/5, SHA)
8. Защита исходного кода программ – обфускация кода.
9. Защита носителей информации (Floppy/HDD/CD/DVD/Flash)
10. Исследование уязвимостей операционных систем
11. Исследование уязвимостей прикладного программного обеспечения
12. Кодирование. Архивация – кодирование сжатием (методы Huffman, Lempel-Ziv, арифметические). Использование кодирования при передаче информации.
13. Комплекс мер по защите информации. Разработка стратегии.
14. Компьютерная разведка. Криптоаналитические атаки.
15. Организационные меры. Физическая, электромагнитная, активная и пассивная защита. Человеческий фактор.
16. Основные моменты гражданского и уголовного кодексов ПМР в отношении защиты информации.
17. Перестановка «Магический квадрат»
18. Разработка комплекса мер по защите информации в рамках организации.
19. Разработка системы защиты программного обеспечения распространяемого по Internet.
20. Разработка собственной криптографической системы.
21. Самотестирующиеся и самокорректирующиеся программы.
22. Симметричные криптосистемы (алгоритмы DES, 3-DES, AES, ГОСТ-28147-89). Принципы работы, назначение.
23. Способы подделки документов и методы выявления подделок.
24. Статистические свойства языка. Вскрытие шифров алфавитной замены.
25. Стеганография. Подготовка и использование симпатических чернил, цифровая стеганография. Методы определения «присутствия» информации.
26. Схема цифровой подписи. Схема шифрования Эль Гамаля.
27. Технические разведки. Компьютерная разведка.
28. Технические разведки. Компьютерная разведка. Методы взлома компьютерных систем. Программы-шпионы.
29. Требования к современным криптографическим системам и алгоритмам.
30. Хакерские атаки, способы борьбы с ними.

Экзаменатор, доцент _____ *Л.Я. Козак*

«УТВЕРЖДАЮ»
зав. кафедрой ИиПИ,
доцент _____ Л.А. Тягульская
«_21__» сентября 2023 г.

Темы индивидуальных заданий
по дисциплине «Защита информации»
для студентов IV курса
направления «Программная инженерия»
профиля подготовки «Разработка программно-информационных систем»,
VII семестр (д/о)

Программа самостоятельной работы по дисциплине «Защита информации» 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 LOKI.
12. Блочный шифр KHUFU.
13. Блочный шифр RC2.
14. Блочный шифр MMB.
15. Блочный шифр SKIPJACK.
16. Блочный шифр SAFER.
17. Блочный шифр 3-WAY.
18. Блочный шифр CRAB.
19. Блочный шифр RC4.
20. Блочный шифр SEAL.
21. Асимметричный ранцевый криптоалгоритм.
22. Асимметричный алгоритм шифрования данных RSA.
23. Асимметричный алгоритм шифрования данных ElGamal.
24. Асимметричный алгоритм шифрования данных Rabin.
25. Асимметричный алгоритм шифрования данных McEliece
26. Алгоритм цифровой подписи с открытым ключом DSA.
27. Алгоритм цифровой подписи с открытым ключом ГОСТ.
28. Однонаправленная хэш-функция *N*-хэш.
29. Однонаправленная хэш-функция MD4, MD5.
30. Алгоритм безопасного хэширования (Secure Hash Algorithm, SHA).

Экзаменатор, доцент _____ Л.Я. Козак

Государственное образовательное учреждение
«ПРИДНЕСТРОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени Т.Г. Шевченко»
Рыбницкий филиал
Кафедра информатики и программной инженерии

Промежуточный тест
по дисциплине «Защита информации»
(наименование дисциплины)

Тест №1
для среза текущих знаний

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 санкционированные.

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 идентифицирующе 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 <u>защитой информации</u> 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 <u>человек,</u> 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 <u>аппаратура,</u> 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 программа, 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) Троянские 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		

Доцент _____ Козак Л.Я.
(подпись) (ФИО)

«_21__» *сентября* *2023* г.

Государственное образовательное учреждение
«ПРИДНЕСТРОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени Т.Г. Шевченко»
Рыбницкий филиал
Кафедра информатики и программной инженерии

Итоговый тест
по дисциплине «Защита информации»
(наименование дисциплины)

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-программные 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		

Доцент _____ *Козак Л.Я.*
(подпись) (ФИО)

«_21_» *сентября* *2023* г.

Государственное образовательное учреждение
«ПРИДНЕСТРОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
имени Т.Г. Шевченко»
Рыбницкий филиал
Кафедра информатики и программной инженерии

Темы рефератов

по дисциплине **«Защита информации»**
(наименование дисциплины)

1. Криптографические протоколы: основные, промежуточные.
2. Криптографические протоколы: развитые, эзотерические.
3. Информационная безопасность автоматизированных систем.
4. Самотестирующиеся и самокорректирующиеся программы.
5. Конфиденциальные вычисления.
6. Системы защиты информации.
7. Развитие теории и практики защиты информации.
8. Сетевая защита.
9. Симметричные криптосистемы.
10. Шифр простой перестановки, магический квадрат
11. **Перестановка «Магический квадрат»**
12. Асимметричные криптосистемы.
13. Хакерские атаки, способы борьбы с ними.
14. Доктрина информационной безопасности ПМР.

Критерии оценки:

- оценка «зачтено» выставляется студенту, если реферат соответствует всем требованиям, предъявляемым к такого рода работам; материал соответствует предлагаемому плану; в реферате раскрывается заявленная тема, решены поставленные задачи; в реферате на основе изучения источников дается самостоятельный анализ фактического материала, делаются самостоятельные выводы; студент демонстрирует свободное владение материалом, уверенно отвечает на основную часть вопросов;

- оценка «не зачтено» - реферат не соответствует всем требованиям, предъявляемым к такого рода работам; материал не соответствует предлагаемому плану; студент не может привести подтверждение теоретическим положениям, не знает источников по теме работы или не может их охарактеризовать; на защите студент не может аргументировать выводы, не отвечает на вопросы; в реферате отсутствуют самостоятельные выводы.

Доцент _____ *Козак Л.Я.*
(подпись) (ФИО)

«_21_» *сентября* *2023* г.