МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РЕСПУБЛИКИ ТАДЖИКИСТАН
МЕЖГОСУДАРСТВЕННОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ»

ЮРИДИЧЕСКИЙ ФАКУЛЬТЕТ
Кафедра Уголовного процесса и криминалистики

«Утверждаю»
Зав. кафедрой уголовного процесса и криминалистики
к.ю.н., доцент _____ Шукурова Н.А
«13» ____11_____2024 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

«Информационная безопасность»

Направление подготовки – 39.03.01 «Социология»

Наименование профиля – «Общая социология»

Форма подготовки – очная

Уровень подготовки - бакалавриат

ДУШАНБЕ - 2024

ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине «Уголовный процесс»
ОБЩИЕ ПОЛОЖЕНИЯ УГОЛОВНОГО ПРОЦЕССА

№ п/п	Контролируемые разделы, темы, модули	Формируемые компетенции	Оценочные средства		
			Индикаторы достижения компетенции	Другие оценочные средства	
				Количество тестовых заданий / вопросов к экзамену / зачету/ зачету (с оценкой)	Вид
1	Тема 1.Международные стандарты информационного обмена. Понятие угрозы. Информационная безопасность в условиях функционирования в России глобальных сетей**.**	**УК-2.** Способен определять круг задач в рамках поставленной целит и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	**ИУК-2.1.** Формулирует в рамках поставленной цели совокупность взаимосвязанных задач, обеспечивающих ее достижение.	10	Круглый стол, дискуссия, полемика, диспут, дебаты
2	Тема 2. Виды противников или «нарушителей». Понятие о видах вирусов.	УК -2	ИУК-2.2. Определяет ресурсное обеспечение для достижения поставленной цели;	10	Эссе
3.	Тема 3. Три вида возможных нарушений информационной системы. Защита.	УК-2	**ИУК-2.3.** Выявляет правовые нормы, предъявляемые к способам решения профессиональных задач, исходя из действующих правовых норм, имеющихся ресурсов и ограничений **ИУК-2.4.** Выполняет задачи в рамках своей ответственности в соответствии с запланированными результатами, при необходимости корректирует способы решения задач	10	Кейс-задание
4.	Тема 4. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы	**ПК-1**. Способен самостоятельно формулировать цели, ставить конкретные задачи научных исследований в различных областях социологии и решать их с помощью современных	**ИПК–1.1.** Использует в профессиональной деятельности базовые и профессионально профилированные знания в области социальных наук; интерпретирует профессиональными терминами и понятиями. **ИПК-1.2.** Использует положения социологической теории и методы социальных наук применительно к целям и задачам		Круглый стол, дискуссия, полемика, диспут, дебаты

		исследовательских методов с использованием новейшего отечественного и зарубежного опыта и с применением современной аппаратуры, оборудования, информационных технологий	фундаментального или прикладного социологического исследования;	10	
5.	Тема 5. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства	ПК-1	**ИПК-1.3.** Применяет новейшие отечественные и зарубежные теоретические, методические и информационные технологии разработки для решения конкретных задач исследований в различных областях социологии.	10	Круглый стол, дискуссия, полемика, диспут, дебаты
6.	Тема 6. Основные положения теории информационной безопасности. Модели безопасности и их применение.	**ПК-4.** Способен составлять и оформлять необходимую документацию, представлять результаты проектной работы с учётом особенностей потенциальной аудитории;	**ИПК-4.1.** Проводит переговоры, взаимодействует с заказчиком фундаментального или прикладного социологического исследования; **ИПК-4.2.** Составляет и оформляет техническую документацию по фундаментальному или прикладному социологическому исследованию. **ИПК-4.3.** Согласовывает с заказчиком содержательных и организационных вопросов фундаментального или прикладного социологического **ИПК-4.4.** Знает основы административного и финансового учета, методы планирования бюджета исследования, стоимость работ, правила, нормы и основные принципы	10	Эссе
7.	Тема 7. Таксономия нарушений информационной безопасности вычислительной системы и причины, обуславливающие их существование	ПК-1	**ИПК-1.1** **ИПК-1.2**	10	Круглый стол, дискуссия, полемика, диспут, дебаты
8.	Тема 8. Анализ способов нарушений информационной безопасности.	ПК-4	**ИПК-4.1** **ИПК-4.2**	10	Эссе
9.	Тема 9. Использование защищенных компьютерных систем.	ПК-4	**ИПК-4.3** **ИПК-4.4**	10	Кейс-задание

10.	Тема 10. Основные технологии построения защищенных систем.	УК - 2	**ИУК-1.1** **ИУК-1.2**	10	Круглый стол, дискуссия, полемика, диспут, дебаты
11	Тема 11. Место информационной безопасности экономических систем в национальной безопасности страны.	УК-2	**ИУК-1.1** **ИУК-1.2**	20	Круглый стол, дискуссия, полемика, диспут, дебаты
	Всего:			120	

МОУ ВО РОССИЙСКО-ТАДЖИКСКИЙ (СЛАВЯНСКИЙ) УНИВЕРСИТЕТ

Юридический факультет
Кафедра уголовного процесса и криминалистики
ТЕСТЫ
по дисциплине «Информационная безопасность»
для направления подготовки – 40.03.01 Юриспруденция
программа подготовки «Уголовное судопроизводство и основы прокурорской деятельности»
форма обучения: очная

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
+ Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
+ Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
+ Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
+ несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
+ Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети

+ Потеря, искажение, утечка информации
7) К основным принципам обеспечения информационной безопасности относится:
+ Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы
8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
+ органы права, государства, бизнеса
- сетевые базы данных, фаерволлы
9) К основным функциям системы безопасности можно отнести все перечисленное:
+ Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей
тест 10) Принципом информационной безопасности является принцип недопущения:
+ Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности
11) Принципом политики информационной безопасности является принцип:
+ Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях
12) Принципом политики информационной безопасности является принцип:
+ Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы
13) Принципом политики информационной безопасности является принцип:
+ Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы
14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
+ Логические закладки («мины»)
- Аварийное отключение питания
15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
+ Удалить письмо с приложением, не раскрывая (не читая) его
16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
+ Секретность закрытого сообщения определяется секретностью ключа
17) ЭЦП – это:
- Электронно-цифровой преобразователь
+ Электронно-цифровая подпись

- Электронно-цифровой процессор
18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО
+ Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов
19) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
+ Сбой (отказ) оборудования, нелегальное копирование данных
20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
+ Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии
21) Утечкой информации в системе называется ситуация, характеризуемая:
+ Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации
22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
+ Целостность
- Доступность
- Актуальностьl
23) Угроза информационной системе (компьютерной сети) – это:
+ Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически
24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной
- Правовой
+ Защищаемой
25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
+ Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные
26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
+ Владелец сети
- Администратор сети
- Пользователь сети
27) Политика безопасности в системе (сети) – это комплекс:
+ Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети
28) Наиболее важным при реализации защитных мер политики безопасности является:
- Аудит, анализ затрат на проведение защитных мер

- Аудит, анализ безопасности
+ Аудит, анализ уязвимостей, риск ситуаций

*полная версия билетов находится на электронном носителе

Перечень оценочных средств

№ п/п	Наименование оценочного средства	Характеристика оценочного средства	Представление оценочного средства в ФОС
1.	Деловая/ ролевая игра	Совместная деятельность группы обучающихся и преподавателя под управлением преподавателя с целью решения учебных и профессионально-ориентированных задач путем игрового моделирования реальной проблемной ситуации. Позволяет оценивать умение анализировать и решать типичные профессиональные задачи.	Тема (проблема): Ожидаемый результат: **Знать:** профессиональные обязанности, основные положения этических и других социальных норм, связанных с деятельностью по обеспечению прав и законных интересов граждан. **Уметь:** добросовестно подходить к выполнению своих профессиональных обязанностей, качественно выполнять поставленные задачи, стремиться к достижению наилучшего результата, избегать конфликта интересов. **Владеть:** навыками поведения юриста, соответствующими требованиям профессиональной этики юриста.
2.	Кейс-задание	Проблемное задание, в котором обучающемуся предлагают осмыслить реальную профессионально-ориентированную ситуацию, необходимую для решения данной проблемы.	Задания для решения кейс-задания Критерии оценки: -соответствие содержания задачи теме; - содержание задачи носит проблемный характер; - решение задачи правильное, демонстрирует применение аналитического и творческого подходов; продемонстрированы умения работы в ситуации неоднозначности и неопределенности; -задача представлена на контроль в срок.
3.	Круглый стол, дискуссия, полемика, диспут, дебаты	Оценочные средства, позволяющие включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения.	**Знать:** содержание норм материального и процессуального права, способы, виды, стадии применения правовых актов, порядок составления и оформления процессуальных документов, основные положения отраслевых юридических и специальных наук, сущность и содержание основных понятий, категорий, институтов, правовых статусов субъектов **Уметь:** использовать нормы материального и процессуального права в профессиональной деятельности, анализировать стадии принятия правовых актов, применять правовые теории, понятия категории в профессиональной деятельности. **Владеть:** навыками работы с нормами процессуального и материального права в профессиональной деятельности, навыками правовой квалификации, установления фактической основы дела, подготовки правоприменительных актов, навыками использования правовых теорий, понятий, категорий в профессиональной деятельности.
4.	Эссе	Средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной проблемы, самостоятельно проводить анализ этой проблемы с использованием концепций и аналитическогод	Критерии оценки: - актуальность темы; -соответствие содержания теме; -глубина проработки материала; - грамотность и полнота использования источников; -соответствие оформления доклада требованиям.

		инструментария соответствующей дисциплины, делать выводы, обобщающие авторскую позицию по поставленной проблеме.	

Приложение

МОУ ВО «Российско-Таджикский» (Славянский) университет»
Кафедра уголовного процесса и криминалистики
ДЕЛОВАЯ (РОЛЕВАЯ) ИГРА
по дисциплине «Информационная безопасность»

1. Принципы организации информационной среды.
2. Понятие информационной безопасности (две трактовки).
3. Ответственность специалиста в области безопасности информации и его функции.
4. Современное состояние информационной безопасности. |
5. Понятие угрозы и характеристика угроз безопасности информации.
6. Несанкционированный доступ (НСД) к информации и его цели.
7. Способы НСД к информации.
8. Три вида возможных нарушений информационной системы: раскрытие, нарушение целостности, отказ в обслуживании.
9. Виды противников или «нарушителей», совершающие компьютерные преступления: хакеры, кракеры и пираты.
10. Компьютерные вирусы и их классификация.
11. Антивирусные программы и их классификация.
12. Понятие защиты информации.
13. Информационная безопасность в условиях функционирования в России глобальных сетей. ,
14. Международные стандарты информационного обмена. t
15. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
16. Назначение и задачи в сфере обеспечения информационной безопасности на уровне государства.
17. Требования к безопасности компьютерных сетей в Российской Федерации.
18. Основные положения теории информационной безопасности корпоративных информационных систем (КИС). I
19. Краткая история создания глобальной информационной сети INTERNET.
20. Стек протоколов TCP/IP. i
21. Проблемы безопасности IP-сетей: варианты распространенных атак на IP-сети и основные причины, порождающие возможность атаки на 1Р-сети.
15
22. Причины уязвимости сети Интернет и сетей и компьютеров, имеющих выход в Интернет.
23. Модель корпоративной сети. I
24. Причины, способствующие атаке информации в корпоративных сетях.
25. Модель угроз и модель противодействия угрозам безопасности корпоративной сети.
26. Место и роль информационной безопасности корпоративных информационных систем (КИС) в национальной безопасности страны.
27. Концепция информационной безопасности в РФ.
28. Защита файлов и папок путем назначения пароля экранной зЬставке,
29. Способы ограничения доступа к информации в MSWord. ,
30. Способы ограничения доступа к информации в MSExcel. '
31. Работа с ключами реестра WindowsXP/7/Ю : создание предупреждающего окна перед входом в систему.
32. Работа с ключами реестра WindowsXP/7/lO: отключение контекстного меню на панели задач и рабочем столе (отключение меню правой кнопки).
33. Понятие браузера. Браузер InternetExplorer.
34. Защита электронной почты от спама.
35. Понятие Cookies. Группы Cookies.
36. Сертификаты безопасности и их виды.
37. Вопросы, на которые нужно ответить, прежде чем

электронной почты.
38. Защита файлов и папок от изменения: только чтение.
39. Защита файлов и папок от изменения: скрытый.
40. Шифрование данных с помощью архиваторов WinRar и PkZi

Приложение 3

Оформление комплекта заданий для контрольной работы
МОУ ВО «Российско-Таджикский» (Славянский) университет»
Кафедра уголовного процесса и криминалистики

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ КОНТРОЛЬНОЙ РАБОТЫ

по дисциплине «Информационная безопасность»

1.Принципы организации информационной среды.
2. Понятие информационной безопасности (две трактовки). !
3. Ответственность специалиста в области безопасности информации и его функции.
4. Современное состояние информационной безопасности.
5. Наступательные и оборонительные составляющие «информационной войны».
6. Понятие угрозы и характеристика угроз безопасности информации.
7. Несанкционированный доступ (НСД) к информации и его цели.
8. Способы НСД к информации. i
9. Три вида возможных нарушений информационной системы: раскрытие, нарушение целостности, отказ в обслуживании.
10. Виды противников или «нарушителей», совершающие компьютерные преступления: хакеры, кракеры и пираты.
11. Компьютерные вирусы и их классификация. I
12. Антивирусные программы и их классификация. Понятие защиты информации.

Приложение 4

МОУ ВО «Российско-Таджикский» (Славянский) университет»
Кафедра уголовного процесса и криминалистики
Перечень дискуссионных тем для круглого стола
(дискуссии, полемики, диспута, дебатов)
по дисциплине «Информационная безопасность»

1. Принципы организации информационной среды.
2. Понятие информационной безопасности (две трактовки).
3. Ответственность специалиста в области безопасности информации и его функции.
4. Современное состояние информационной безопасности. |
5. Понятие угрозы и характеристика угроз безопасности информации.
6. Несанкционированный доступ (НСД) к информации и его цели.
7. Способы НСД к информации.
8. Три вида возможных нарушений информационной системы: раскрытие, нарушение целостности, отказ в обслуживании.
9. Виды противников или «нарушителей», совершающие компьютерные преступления: хакеры, кракеры и пираты.
10. Компьютерные вирусы и их классификация.
11. Антивирусные программы и их классификация.
12. Понятие защиты информации.
13. Информационная безопасность в условиях функционирования в России глобальных сетей. ,
14. Международные стандарты информационного обмена. t
15. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.

Критерии оценки:

Максимальное количество баллов, указанное по каждому виду задания, студент получает, если:

- обстоятельно с достаточной полнотой излагает соответствующую тему;
- даёт правильные формулировки, точные определения, понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания студентом данного материала.

70~89% от максимального количества баллов студент получает, если:

- неполно (не менее 70% от полного), но правильно изложено задание;
- при изложении были допущены 1-2 несущественные ошибки, которые он исправляет после замечания преподавателя;
- даёт правильные формулировки, точные определения,понятия терминов;
- может обосновать свой ответ, привести необходимые примеры;
- правильно отвечает на дополнительные вопросы преподавателя, имеющие целью выяснить степень понимания студентомданного материала.

50~69% от максимального количества баллов студент получает, если:

- неполно (не менее 50% от полного), но правильно изложено задание;
- при изложении была допущена 1 существенная ошибка;
- знает и понимает основные положения данной темы, нодопускает неточности в формулировке понятий;
- излагает выполнение задания недостаточно логично и последовательно;
- затрудняется при ответах на вопросы преподавателя.
- 49% и менее от максимального количества баллов студент получает, если:
- неполно (менее 50% от полного) изложено задание;
- при изложении были допущены существенные ошибки.

В "0" баллов преподаватель вправе оценить выполненное студентом задание, если оно не удовлетворяет требованиям, установленным преподавателем к данному виду работы.

Сумма полученных баллов по всем видам заданий внеаудиторной самостоятельной работы составляет рейтинговый показатель студента. Рейтинговый показатель студента влияет на выставление итоговой оценки по результатам изучения дисциплины.

Приложение 7.5.

МОУ ВО «Российско-Таджикский (Славянский) университет»
Кафедра Уголовного процесса и криминалистики

ТЕМЫ ЭССЕ
(рефератов, докладов, сообщений)
по дисциплине «Информационная безопасность»
Темы рефератов:

Принципы организации информационной среды.
2. Понятие информационной безопасности (две трактовки).
3. Понятие угрозы и характеристика угроз безопасности информации.
4. Несанкционированный доступ (НСД) к информации и его цели.
5. Виды противников или «нарушителей», совершающие компьютерные преступления: хакеры, кракеры и пираты.
6. Компьютерные вирусы и их классификация.
7. Антивирусные программы и их классификация.
8. Понятие защиты информации.
9. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. |
10. Основные положения теории информационной безопасности корпоративных информационных систем (КИС).
11. Стек протоколов TCP/IP.
12. Причины уязвимости сети Интернет и сетей и компьютеров, имеющих выход в Интернет.
13. Модель корпоративной сети.
14. Концепция информационной безопасности в РФ.
15. Перспективные технологии информационной защиты корпоративных информационных систем (КИС) и концепция построения защищенных виртуальных частных сетей VPN.

16. Функции и компоненты сети VPN и критерии ее безопасности.
17. Об истории развития криптографии (шифр «Скитала» в Спарте, шифр Цезаря, квадрат Полибия, шифр Гронсфельда).
18. Основные понятия криптографии. I
19. Симметричные алгоритмы шифрования: понятия блочного и поточного шифров.
20. Обобщенная схема работы симметричной криптосистемы.
21. Отечественный стандарт шифрования данных ГОСТ 28147-89: режимы работы, схема реализации шифрования и расшифрования данных в режиме простой замены.
22. Общий вид уравнений шифрования данных в режиме простой замены в отечественном стандарте ГОСТ 28147-89. |
23. Уравнения расшифрования в режиме простой замены в отечественном стандарте ГОСТ 28147-89.
24. Основные свойства асимметричных криптосистем.
25. Однонаправленные функции.
26. Алгоритм шифрования RSA.
27. Понятие хэш-функции и ее свойства.
28. Понятие электронной цифровой подписи и ее цель
29. Процедура формирования и проверки ЭЦП.
30. Алгоритмы электронной цифровой подписи - RSA: основные сведения.
31. Отечественный стандарт ЭЦП.

Критерии оценки:

Оценка «зачтено» выставляется студенту, если **присутствует:**
- актуальность темы исследования;
- соответствие содержания теме;
- глубина проработки материала;
- правильность и полнота разработки поставленных вопросов;
- значимость выводов для дальнейшей практической деятельности;
- правильность и полнота использования литературы;
- соответствие оформления реферата стандарту;
- качество сообщения и ответов на вопросы при защите реферата.

К примеру, объем реферата может колебаться в пределах 15-20 печатных страниц. Основные разделы: оглавление (план), введение, основное содержание, заключение, список литературы.

Текст реферата должен содержать следующие разделы:
- титульный лист с указанием: названия ВУЗа, кафедры, темы реферата, ФИО автора и ФИО научного руководителя.
- введение, актуальность темы.
- основной раздел.
- заключение (анализ результатов литературного поиска); выводы.
- библиографическое описание, в том числе и интернет-источников.
- список литературных источников должен иметь не менее 10 библиографических названий, включая сетевые ресурсы.

Текстовая часть реферата оформляется на листе следующего формата:
- отступ сверху – 2 см; отступ слева – 3 см; отступ справа – 1,5 см; отступ снизу – 2,5 см;
- шрифт текста: Times New Roman, высота шрифта – 14, пробел – 1,5;
- нумерация страниц – снизу листа. На первой странице номер не ставится.

Реферат должен быть выполнен грамотно с соблюдением культуры изложения. Обязательно должны иметься ссылки на используемую литературу, включая периодическую литературу за последние 5 лет.

Доклад – вид самостоятельной научно-исследовательской работы, где обучающийся раскрывает суть исследуемой проблемы; приводит различные точки зрения, а также собственные взгляды на нее.

Этапы работы над докладом:
- подбор и изучение основных источников по теме (как и при написании реферата рекомендуется использовать не менее 8 - 10 источников);
- составление библиографии;
- обработка и систематизация материала, подготовка выводов и обобщений.
- разработка плана доклада.
- написание;
- публичное выступление с результатами исследования.

Если студент готовить доклад, то самостоятельная работа по их написанию может проходить в следующей последовательности.

1. Нужно проконсультироваться у преподавателя по содержанию предстоящего доклада (выступления), списку литературы, которую лучше использовать для их подготовки. Подобрать рекомендованную литературу.
2. Необходимо изучить литературу, сгруппировать материал и составить подробный план доклада (выступления).
3. Следует написать полный текст доклада (выступления). Для того чтобы доклад получился интересным и имел успех, в нем следует учесть:
а) теоретическое содержание рассматриваемых вопросов и их связь с практикой профессиональной деятельности;
б) логику и аргументы высказываемых суждений и предложений, их остроту и актуальность;
в) конкретные примеры из сферы профессиональной или учебной деятельности;
г) обобщающие выводы по всему содержанию сделанного доклада с выходом на будущую профессию.
Для выступления с докладом студенту отводится 10 – 12 минут, поэтому все содержание доклада должно быть не более 7-10 страниц рукописного текста. Для выступления с сообщением обычно отводится 5-7 минут. Соблюдение регламента времени является обязательным условием.
4. Студенту рекомендуется продумать методику чтения доклада. Лучше если студент будет свободно владеть материалом и излагать доклад доходчивым разговорным языком, поддерживать контакт с аудиторией. При возможности следует применять технические средства, наглядные пособия (например, подготовить доклад с презентацией или раздаточным материалом), использовать яркие примеры.
Важно потренироваться в чтении доклада. Если есть возможность, то записать свое выступление на видео - или аудионоситель. Просмотр, прослушивание сделанной записи позволят увидеть и устранить недостатки: неправильное произношение слов, несоответствующий темп речи, ошибки в ударении, неинтересные или непонятные места, продолжительность доклада и т.п.
Критерии оценки:
- актуальность темы;
- соответствие содержания теме;
- глубина проработки материала;
- грамотность и полнота использования источников;
- соответствие оформления доклада требованиям.
- оценка «не зачтено» выставляется студенту в случае, если он не ориентируется в теме подготовленного реферата, доклада, эссе.

Разработчик:_____ Назарзода Р.Г.