МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д. МИЛЛИОНЩИКОВА»

Кафедра «Юриспруденция»

УТВЕРЖДЕН
на заседании кафедры
« 22 » 06 2025 г., протокол № 4
и.о. Зав. кафедрой

_____ М.Р. Богатырев

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

Киберпреступность и информационная безопасность

Направление подготовки

40.04.01 «*Юриспруденция*»

Направленность (профиль)

«Юриспруденция»

Квалификация

Магистр

Составитель: _____ М.Р. Богатырев

Грозный – 2025

ПАСПОРТ
ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ
Киберпреступность и информационная безопасность

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Основные законы и понятия современного информационного оборота.	ПК-2	Тестовые задания; реферат
2.	Современная криминологическая оценка преступлений в сфере компьютерной информации.	ПК-5	Тестовые задания; реферат
3.	Уголовно-правовая характеристика преступлений в сфере компьютерной информации по УК РФ	ПК-2	Тестовые задания; реферат
4.	Виды преступлений и опасных деяний в сфере обращения цифровой информации, нуждающихся в криминализации.	ПК-2	Тестовые задания; реферат
5.	Вопросы квалификации преступлений в сфере компьютерной информации.	ПК-5	Тестовые задания; реферат
6.	Состояние и тенденции развития зарубежного и международного уголовного законодательства в сфере защиты компьютерной информации.	ПК-5	Тестовые задания; реферат
7.	Причины и условия преступлений в сфере компьютерной информации. Особенности личности компьютерного преступника.	ПК-5	Тестовые задания; реферат
8.	Основные направления и меры борьбы с преступлениями в сфере компьютерной информации в РФ.	ПК-5	Тестовые задания; реферат

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1	Тест	Средство проверки полученных знаний по пройденным темам или разделам учебной дисциплины.	Комплект тестовых заданий

2	Реферат	Продукт самостоятельной работы студента, представляющий собой публичное выступление по решению определенной учебно-практической, учебно- исследовательской или научной темы.	Темы рефератов
3	Зачет	Промежуточная форма оценки	Комплект билетов к зачету

Темы рефератов

1. Научно-технический прогресс и его последствия (побочные эффекты).
2. Основные законы и понятия современного информационного оборота.
3. Современная криминологическая оценка преступлений в сфере компьютерной информации.
4. Уголовно-правовая характеристика преступлений в сфере компьютерной информации по УК РФ.
5. Иные виды преступлений и опасных деяний в сфере обращения цифровой информации, нуждающихся в криминализации.
6. Вопросы квалификации преступлений в сфере компьютерной информации.
7. Общая характеристика и виды преступлений в сфере компьютерной информации по уголовному законодательству зарубежных стран.
8. Типология личности преступника в сфере компьютерной информации.
9. Правовое регулирование борьбы с преступлениями в сфере компьютерной информации.
10. Меры предупреждения преступлений в сфере компьютерной информации.
11. Виктимологическая профилактика преступлений в сфере компьютерной информации.
12. Система субъектов, осуществляющих борьбу с преступлениями в сфере компьютерной информации.
13. Создание, использование и распространение вредоносных программ.
14. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации.
15. Уголовная ответственность за неправомерное воздействие на критическую информационную инфраструктуру.
16. Мошенничество в сфере компьютерной информации: способы совершения и доказательства.
17. Фишинг как вид кибермошенничества: технологии и защита от него.
18. Криптоджекинг и его правовая квалификация.
19. Утечки персональных данных: правовой режим защиты и ответственность.
20. Обеспечение информационной безопасности в органах государственной власти.

21. Правовой статус субъектов критической информационной инфраструктуры в Российской Федерации.

22. Доказывание и особенности проведения судебной компьютерно-технической экспертизы.

23. Будапештская конвенция о киберпреступности.

24. Противодействие кибертерроризму и пропаганде экстремизма в сети Интернет.

25. Использование технологий искусственного интеллекта для совершения киберпреступлений.

Критерии оценивания рефератов

- ***0 баллов выставляется студенту, если*** *подготовлен некачественный реферат: тема не раскрыта*, в изложении отсутствует четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений.

- 1- балл выставляется студенту, если *подготовлен некачественный реферат: тема раскрыта, однако в изложении отсутствует четкая структура,* отражающая сущность раскрываемых понятий, теорий, явлений.

- 2 балла выставляется студенту, если *подготовлен качественный реферат:* тема хорошо раскрыта, в изложении прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. *Однако студент недостаточно владеет подготовленным материалом.*

- 3 балла выставляется студенту, если *подготовлен качественный реферат:* тема хорошо раскрыта, в изложении прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. *Студент хорошо апеллирует терминами науки. Однако затрудняется ответить на дополнительные вопросы по теме реферата (1-2 вопроса).*

- 4 балла выставляется студенту, если *подготовлен качественный реферат:* тема хорошо раскрыта, в изложении прослеживается четкая структура логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. *Студент свободно апеллирует терминами науки. Однако на дополнительные вопросы по теме реферата (1-2 вопроса) отвечает только с помощью преподавателя.*

- 5 баллов выставляется студенту, если *подготовлен качественный реферат:* тема хорошо раскрыта, в изложении прослеживается четкая структура логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. *Студент свободно апеллирует терминами науки, демонстрирует авторскую позицию. Способен ответить на дополнительные вопросы по теме реферата (1-2 вопроса).*

КОНТРОЛЬНО-ИЗМЕРИТЕЛЬНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ

«Киберпреступность и информационная безопасность»

Вопросы к зачету

1. Развитие техники как прогресс и источник социальных проблем.
2. Влияние НТП на соотношение умышленной и неосторожной преступности.
3. Возможности и пределы влияния уголовного законодательства на технический прогресс.
4. Значение информации в жизни социума.
5. Компьютерная форма информации, ее достоинства и проблемы пользования. Свобода и ограничения в пользовании информацией.
6. Понятийный ряд электронного (компьютерного) оборота.
7. Нормативная основа, регулирующая оборот компьютерной информации в современном обществе.
8. Информация как очевидный объект криминальных посягательств.
9. Хакерские атаки и компьютерные вирусы.
10. Криминологическая характеристика современной компьютерной преступности в России и за рубежом.
11. Основной состав преступления в виде неправомерного доступа к компьютерной информации (ст.272 УК РФ).
12. Можно ли считать компьютерную информацию предметом преступления, а компьютерные посягательства относить к категории материальных составов?
13. Значение примечаний к ст. 272 УК РФ.
14. Понятие вредоносных компьютерных программ и способы их распространения (ст.273 УК РФ).
15. «Материальность» состава и виды обязательных последствий (уничтожение, блокирование, модификация, копирование или нейтрализация средств защиты компьютерной информации) (ст.273 УК РФ).
16. Понятие и значение признака «заведомости» в сознании автора вредоносных компьютерных программ (ст.273 УК РФ).
17. Характеристика квалифицирующих признаков состава преступления «Создание, использование и распространение вредоносных компьютерных программ» (ст.273 УК РФ).
18. Объект, объективная сторона, субъект и субъективная сторона состава нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно- телекоммуникационных сетей (ст.274 УК РФ).
19. Уголовно-правовая характеристика ст. 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».
20. Уголовно-правовая характеристика ст. 274.2 УК РФ «Нарушение правил централизованного управления техническими средствами противодействия угрозам

устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования».

21. Бланкетная основа уголовной ответственности за компьютерное преступление.

22. Понятие информационно-телекоммуникационных сетей.

23. Причины и условия как детерминанты преступности.

24. Личность компьютерного преступника.

25. Предупреждение компьютерной преступности и профилактика компьютерных преступлений.

Тестовые задания к текущему контролю по дисциплине
«Киберпреступность и информационная безопасность»
Первая текущая аттестация:

1.Развитие техники как прогресс и источник социальных проблем:
a) Техника всегда улучшает качество жизни и не вызывает проблем.
b) Развитие техники приводит исключительно к экономическому росту.
c) Техника может создавать новые социальные проблемы, такие как безработица и зависимость от технологий.

2.Влияние НТП на соотношение умышленной и неосторожной преступности:
a) НТП увеличивает только умышленные преступления.
b) НТП увеличивает количество неосторожных преступлений.
c) НТП влияет на оба типа преступлений, но сложно предсказать как.

3.Возможности и пределы влияния уголовного законодательства на технический прогресс:
a) Уголовное законодательство всегда тормозит технический прогресс.
b) Уголовное законодательство может как тормозить, так и стимулировать технический прогресс.
c) Уголовное законодательство не влияет на технический прогресс.

4.Значение информации в жизни социума:
a) Информация важна только для ученых и специалистов.
b) Информация играет ключевую роль в повседневной жизни и экономике.
c) Информация не имеет большого значения для большинства людей.

5.Компьютерная форма информации, ее достоинства и проблемы пользования:
a) Компьютерная информация удобна и не имеет недостатков.
b) Компьютерная информация имеет множество достоинств, но также проблемы безопасности и доступности.
c) Компьютерная информация неудобна в использовании и имеет много ограничений.

6.Понятийный ряд электронного (компьютерного) оборота:
a) Включает только технические термины.
b) Включает юридические и технические термины.
c) Включает только юридические термины.

7.Нормативная основа, регулирующая оборот компьютерной информации:
a) Регулируется только гражданским правом.
b) Регулируется уголовным и административным правом.
c) Регулируется только международным правом.

8.Информация как объект криминальных посягательств:
a) Информация не может быть объектом преступления.
b) Информация может быть объектом преступлений, таких как хакерские атаки.
c) Информация важна только для экономических преступлений.

9.Хакерские атаки и компьютерные вирусы:
a) Это одно и то же.
b) Хакерские атаки включают в себя использование вирусов.
c) Хакерские атаки могут включать или не включать вирусы.

10.Криминологическая характеристика современной компьютерной преступности:
a) Преобладает в развитых странах.
b) Растет как в развитых, так и в развивающихся странах.
c) Преобладает в странах с низким уровнем технологического развития.

Вариант 2

1.**Понятийный ряд электронного (компьютерного) оборота:**
a) Включает только правовые термины.
b) Включает технические и правовые термины.
c) Включает только технические термины.

2.Нормативная основа, регулирующая оборот компьютерной информации:
a) Регулируется только международными актами.
b) Регулируется только национальным законодательством.
c) Регулируется как национальным, так и международным правом.

3.Информация как очевидный объект криминальных посягательств:
a) Информация не может быть объектом преступления.
b) Информация может быть объектом преступлений.
c) Только экономическая информация важна для преступлений.

4.Хакерские атаки и компьютерные вирусы:
a) Всегда связаны с вредоносными программами.
b) Могут быть без использования вирусов.
c) Это одно и то же.

5.Криминологическая характеристика современной компьютерной преступности в России и за рубежом:
a) Преобладает в России.
b) Преобладает за рубежом.
c) Растет в обоих регионах.

6.Основной состав преступления в виде неправомерного доступа к компьютерной информации (ст.272 УК РФ):
a) Включает только физическое проникновение.
b) Включает доступ без разрешения.
c) Включает только копирование данных.

7.Можно ли считать компьютерную информацию предметом преступления:
a) Нет, это не материальный объект.
b) Да, это материальный объект.
c) Только в некоторых случаях.

8.Значение примечаний к ст. 272 УК РФ:
a) Усиливают наказание.
b) Облегчают квалификацию.
c) Не имеют значения.

9.Понятие вредоносных компьютерных программ и способы их распространения (ст.273 УК РФ):
a) Только через интернет.
b) Через интернет и физические носители.
c) Только через физические носители.

10.Понятие и значение признака «заведомости» в сознании автора вредоносных компьютерных программ (ст.273 УК РФ):
a) Не имеет значения.

b) Усиливает ответственность.
c) Облегчает ответственность.

Вторая текущая аттестация:
Вариант 1

1. Какой из примеров иллюстрирует негативное социальное последствие развития цифровых технологий?
a) Рост производительности труда благодаря автоматизации.
b) Увеличение числа безработных из-за замены людей роботами на производстве.
c) Ускорение коммуникации между людьми по всему миру.

2. Какое явление чаще всего приводит к неосторожным преступлениям в сфере информационных технологий?
a) Целенаправленный взлом корпоративной сети хакерами.
b) Случайная отправка конфиденциальных данных не тому адресату из-за невнимательности сотрудника.
c) Создание и распространение вредоносного ПО.

3. Какой механизм позволяет уголовному законодательству стимулировать развитие безопасных технологий?
a) Полный запрет на разработку экспериментального ПО.
b) Введение уголовной ответственности за утечки данных, что мотивирует компании инвестировать в кибербезопасность.
c) Запрет на использование открытого исходного кода.

4. Какая функция информации наиболее важна для демократического общества?
a) Коммерческая (продажа данных).
b) Контрольная (информирование граждан о деятельности власти).
c) Развлекательная.

5. Что относится к правовым ограничениям свободы информации в РФ?
a) Запрет на распространение материалов, содержащих призывы к экстремизму.
b) Запрет на публикацию любых критических статей о правительстве.
c) Обязательная предварительная цензура всех интернет-публикаций.

6. Какой термин описывает юридически значимый обмен документами в электронной форме?
a) Цифровая подпись.
b) Электронный документооборот.
c) Облачное хранилище.

7. Какой нормативный акт в РФ является базовым для регулирования оборота компьютерной информации?
a) Уголовный кодекс РФ.
b) Федеральный закон «Об информации, информационных технологиях и о защите информации».
c) Трудовой кодекс РФ.

8. Что является типичным объектом атаки при краже персональных данных?
a) Личные фотографии в облачном хранилище.
b) Базы данных операторов связи или банков.
c) Публичные страницы в социальных сетях.

9. Какая мера наиболее эффективна против распространения компьютерных вирусов?
a) Использование антивирусного ПО и регулярное обновление ОС.
b) Полный отказ от интернета.
c) Хранение всех данных исключительно на бумажных носителях.

10. Какой фактор является ключевым в профилактике компьютерной преступности?
a) Увеличение количества камер видеонаблюдения в городах.
b) Повышение цифровой грамотности населения и обучение кибербезопасности.
c) Запрет на продажу персональных компьютеров.

Вариант 2

1. Какой социальный эффект относится к негативным последствиям автоматизации производства?
a) Сокращение рутинного труда и повышение квалификации работников.
b) Рост структурной безработицы из-за исчезновения ряда профессий.
c) Увеличение средней заработной платы во всех отраслях.

2. Какой вид преступления чаще всего возникает из-за недостаточной цифровой грамотности пользователя?
a) Фишинг, совершённый злоумышленником.
b) Случайная утечка данных из-за перехода по вредоносной ссылке.
c) Целенаправленный взлом корпоративной сети.

3. Какое ограничение уголовного законодательства может сдерживать инновации в IT-сфере?
a) Запрет на использование иностранных облачных сервисов.
b) Чрезмерно широкие формулировки составов преступлений (например, «неправомерный доступ»), создающие правовую неопределённость.
c) Обязательная сертификация ПО для всех стартапов.

4. Какая характеристика информации определяет её ценность в современном обществе?
a) Объём данных в байтах.
b) Актуальность и достоверность.
c) Способ хранения (бумажный/электронный).

5. Какое ограничение свободы информации прямо закреплено в Конституции РФ?
a) Запрет на распространение сведений, составляющих государственную тайну.
b) Запрет критики государственных органов в СМИ.
c) Обязательное согласование публикаций с администрацией президента.

6. Что означает термин «электронная подпись» в юридическом контексте?
a) Сканированная копия собственноручной подписи.
b) Реквизит электронного документа, позволяющий подтвердить его авторство и неизменность.
c) Пароль для входа в личный кабинет на сайте.

7. Какой нормативный акт устанавливает базовые принципы защиты персональных данных в РФ?
a) Уголовный кодекс РФ.
b) Федеральный закон «О персональных данных» (№ 152-ФЗ).
c) Трудовой кодекс РФ.

8. Что является наиболее частой целью киберпреступников при атаках на организации?
a) Кража офисной техники.
b) Получение доступа к финансовым данным и счетам.
c) Размещение рекламы на сайте компании.

9. Какой тип хакерской атаки направлен на перехват и изменение данных в процессе передачи?
a) DDoS-атака.
b) Атака типа «человек посередине» (Man-in-the-Middle).
c) Фишинговая рассылка.

10. Какой фактор способствует росту транснациональной компьютерной преступности?

a) Единые стандарты кибербезопасности во всех странах.
b) Анонимность и трансграничность интернета.
c) Полное отсутствие международного сотрудничества в сфере кибербезопасности.

Критерии оценки выполнения тестовых заданий:

- 0 баллов – задание не выполнено (не найдено правильное решение).

- 5 баллов - задание выполнено на 50%

- 10 -баллов – задание выполнено на 100% (найдено правильное решение).

Баллы за тесты выводятся по следующему критерию - в каждом варианте тестов - 10 вопросов - 1 балл за каждый верный ответ.

Ключи к тестовым заданиям

№	Первая текущая аттестация		Вторая текущая аттестация	
	Вариант №1	**Вариант №2**	**Вариант №1**	**Вариант №2**
1	C	B	B	B
2	B	C	B	B
3	B	B	B	B
4	B	B	B	B
5	B	C	A	A
6	B	B	B	B
7	B	A	B	B
8	B	B	B	B
9	C	B	A	B
10	B	B	B	B

Комплект билетов к зачету

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 1

1. Развитие техники как прогресс и источник социальных проблем.

2. Основной состав преступления в виде неправомерного доступа к компьютерной информации (ст.272 УК РФ).

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 2

1. Криминологическая характеристика современной компьютерной преступности в России и за рубежом.

2. Понятие и значение признака «заведомости» в сознании автора вредоносных компьютерных программ (ст.273 УК РФ).

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 3

1. «Материальность» состава и виды обязательных последствий (уничтожение, блокирование, модификация, копирование или нейтрализация средств защиты компьютерной информации) (ст.273 УК РФ).

2. Характеристика квалифицирующих признаков состава преступления «Создание, использование и распространение вредоносных компьютерных программ» (ст.273 УК РФ).

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 4

1. Предупреждение компьютерной преступности и профилактика компьютерных преступлений.

2. Причины и условия как детерминанты преступности.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 5

1. Влияние НТП на соотношение умышленной и неосторожной преступности.

2. Значение информации в жизни социума.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 6

1. Понятие информационно-телекоммуникационных сетей.

2. Информация как очевидный объект криминальных посягательств.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 7

1. Влияние НТП на соотношение умышленной и неосторожной преступности.

2. Понятие и значение признака «заведомости» в сознании автора вредоносных компьютерных программ (ст.273 УК РФ).

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 8

1. Уголовно-правовая характеристика ст. 274.1 УК РФ «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации».

2. Криминологическая характеристика современной компьютерной преступности в России и за рубежом.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 9

1. Характеристика квалифицирующих признаков состава преступления «Создание, использование и распространение вредоносных компьютерных программ» (ст.273 УК РФ).

2. Значение примечаний к ст. 272 УК РФ.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 10

1. Личность компьютерного преступника.

2. Значение информации в жизни социума.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 11

1. Объект, объективная сторона, субъект и субъективная сторона состава нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно- телекоммуникационных сетей (ст.274 УК РФ).

2. Влияние НТП на соотношение умышленной и неосторожной преступности.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 12

1. Компьютерная форма информации, ее достоинства и проблемы пользования. Свобода и ограничения в пользовании информацией.

2. Криминологическая характеристика современной компьютерной преступности в России и за рубежом.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 13

1. Возможности и пределы влияния уголовного законодательства на технический прогресс.

2. Понятийный ряд электронного (компьютерного) оборота.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 14

1. Развитие техники как прогресс и источник социальных проблем.

2. Понятие информационно-телекоммуникационных сетей.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 15

1. Компьютерная форма информации, ее достоинства и проблемы пользования. Свобода и ограничения в пользовании информацией.

2. Понятие и значение признака «заведомости» в сознании автора вредоносных компьютерных программ (ст.273 УК РФ).

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 16

1. Значение информации в жизни социума.

2. Объект, объективная сторона, субъект и субъективная сторона состава нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно- телекоммуникационных сетей (ст.274 УК РФ).

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 17

1. Криминологическая характеристика современной компьютерной преступности в России и за рубежом.

2. Предупреждение компьютерной преступности и профилактика компьютерных преступлений.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 18

1. Объект, объективная сторона, субъект и субъективная сторона состава нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно- телекоммуникационных сетей (ст.274 УК РФ).

2. Личность компьютерного преступника.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 19

1. Бланкетная основа уголовной ответственности за компьютерное преступление.

2. Возможности и пределы влияния уголовного законодательства на технический прогресс.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 20

1. Значение информации в жизни социума.

2. Понятие информационно-телекоммуникационных сетей.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 21

1. Развитие техники как прогресс и источник социальных проблем.

2. Причины и условия как детерминанты преступности.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 22

1. Объект, объективная сторона, субъект и субъективная сторона состава нарушения правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно- телекоммуникационных сетей (ст.274 УК РФ).

2. Понятие информационно-телекоммуникационных сетей.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 23

1. Нормативная основа, регулирующая оборот компьютерной информации в современном обществе.

2. Значение информации в жизни социума.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 24

1. Бланкетная основа уголовной ответственности за компьютерное преступление.

2. Развитие техники как прогресс и источник социальных проблем.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр ""
Дисциплина Киберпреступность и информационная безопасность"
Билет № 25

1. Понятие вредоносных компьютерных программ и способы их распространения (ст.273 УК РФ).

2. Причины и условия как детерминанты преступности.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

Критерии оценивания:

Уровень знаний определяется оценками «отлично», «хорошо», «удовлетворительно», «неудовлетворительно».

Оценка **«отлично»** - студент показывает полные и глубокие знания программного материала, логично и аргументировано отвечает на поставленный вопрос, а также дополнительные вопросы, показывает высокий уровень теоретических знаний.

Оценка **«хорошо»** - студент показывает глубокие знания программного материала, грамотно его излагает, достаточно полно отвечает на поставленный вопрос и дополнительные вопросы, умело формулирует выводы. В тоже время при ответе допускает несущественные погрешности.

Оценка **«удовлетворительно»** - студент показывает достаточные, но не глубокие знания программного материала; при ответе не допускает грубых ошибок или противоречий, однако в формулировании ответа отсутствует должная связь между анализом, аргументацией и выводами. Для получения правильного ответа требуется уточняющие вопросы.

Оценка **«неудовлетворительно»** - студент показывает недостаточные знания программного материала, не способен аргументировано и последовательно его излагать, допускается грубые ошибки в ответах, неправильно отвечает на поставленный вопрос или затрудняется с ответом.