МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

имени академика М.Д. Миллионщикова

«УТВЕРЖДАЮ»

Первый проректор – проректор ОД

_____ И.Г. Гайрабеков

«23» 04 2026г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Киберпреступность и информационная безопасность»

Направление подготовки

40.03.01 Юриспруденция

профиль

«Юриспруденция»

Квалификация

Магистр

Грозный – 2026

1. Цели и задачи дисциплины

1.1 Целью изучения дисциплины является изучение теоретических и практических вопросов обеспечения информационной безопасности общества и государства в новых технологических условиях, вопросов борьбы с киберпреступностью, формирование у студентов навыков юридического сопровождения процессов, связанных с обеспечением информационной безопасности и противодействия киберпреступлениям.

1.2. Задачи изучения дисциплины:

– **Сформировать системное понимание** современной киберпреступности как транснациональной угрозы, ее основных видов, тенденций и социально-правовых последствий.

– **Обеспечить усвоение норм** национального и международного права, регулирующих вопросы информационной безопасности и борьбы с киберпреступлениями.

– **Раскрыть особенности производства по уголовным делам** данной категории, включая специфику проведения следственных действий, работы с цифровыми доказательствами и назначения судебных экспертиз.

– **Развить практические навыки** анализа правовых ситуаций (кейсов), составления процессуальных документов и применения правовых механизмов защиты от киберугроз.

2. Место дисциплины в структуре образовательной программы:

Дисциплина ««**Киберпреступность и информационная безопасность**» относится к обязательным дисциплинам. К началу изучения данной дисциплины студенты должны обладать соответствующими знаниями по дисциплинам «Теория государства и права», «Уголовное право», «Уголовный процесс», «Административное право», «Международное право» и др. Знания, умения и навыки, сформированные при изучении дисциплины «**Киберпреступность и информационная безопасность**», могут быть использованы при прохождении производственной практики.

3. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с индикаторами достижения компетенций:

Таблица 1

Код по ФГОС	**Индикаторы достижения**	**Планируемые результаты обучения по дисциплине**
Профессиональные		
ПК-2. Способен квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности, реализовывать нормы материального и	ПК-2.1. Имеет представление об основных юридических понятиях и категориях, необходимых для реализации норм права в юридической деятельности ПК-2.2. Применяет нормативные правовые акты в профессиональной	Знать: нормы материального и процессуального права. Уметь: реализовать нормы материального и процессуального права в профессиональной деятельности.

процессуального права в профессиональной деятельности	деятельности	Владеть: навыками работы с правовыми актами, на основе их анализа принимает решения о реализации норм материального и процессуального права в профессиональной деятельности.
ПК-5. Способен защищать права и законные интересы субъектов права	ПК-5.1. Понимает механизм защиты прав и законных интересов субъектов права ПК-5.2. Применяет различные способы защиты прав и законных интересов субъектов права	Знать: законодательство в сфере информационных технологий, киберпреступности, формы и способы защиты нарушенных прав и особенности их применения Уметь: применять нормы закона в области информационной безопасности. Владеть: навыками анализа и применения нормативных правовых актов в сфере информационной безопасности.

4. Объем дисциплины и виды учебной работы

Таблица 2

Вид учебной работы	**Всего часов/ зач.ед.**			**Семестры**		
				1	**1**	**1**
	ОФО	**ОЗФО**	**ЗФО**	**ОФО**	**ОЗФО**	**ЗФО**
Контактная работа (всего)	**30/0,83**	**30/0,83**	**12/0,33**	**30/0,083**	**30/0,83**	**12/0,33**
В том числе:						
Лекции	15/0,41	15/0,41	6/0,16	15/0,41	15/0,41	6/0,16
Практические занятия	15/0,41	15/0,41	6/0,16	15/0,41	15/0,41	6/0,16
Самостоятельная работа (всего)	**78/2,16**	**78/2,16**	**96/2,6**	**78/2,16**	**78/2,16**	**96/2,6**
В том числе:						
Темы для самостоятельного изучения	36/1	36/1	32/0,8	36/1	36/1	32/0,8

Подготовка к реферату		24/0,66	24/0,66	32/0,8	24/0,66	24/0,66	32/0,8
Подготовка к зачету		18/0,5	18/0,5	32/0,8	18/0,5	18/0,5	32/0,8
Вид промежуточной аттестации		**зачет**	**зачет**	**зачет**	**зачет**	**зачет**	**зачет**
Общая трудоемкость дисциплины	**ВСЕГО в часах**	**108**	**108**	**108**	**108**	**108**	**108**
	ВСЕГО в зач. единицах	**3**	**3**	**3**	**3**	**3**	**3**

5. Содержание дисциплины

5.1. Разделы дисциплины и виды занятий

Таблица 3

№ п/п	Наименование раздела дисциплины	Часы лекционных занятий			Часы практических занятий		
		ОФО	ОЗФО	ЗФО	ОФО	ОЗФО	ЗФО
1.	Основные законы и понятия современного информационного оборота.	2	2	-	2	2	-
2.	Современная криминологическая оценка преступлений в сфере компьютерной информации.	2	2	2	2	2	2
3.	Уголовно-правовая характеристика преступлений в сфере компьютерной информации по УК РФ	2	2	-	2	2	-
4.	Виды преступлений и опасных деяний в сфере обращения цифровой информации, нуждающихся в криминализации.	2	2	2	2	2	2
5.	Вопросы квалификации преступлений в сфере компьютерной информации.	2	2	-	2	2	-
6.	Состояние и тенденции развития зарубежного и международного уголовного законодательства в сфере защиты компьютерной информации.	2	2	-	2	2	-
7.	Причины и условия преступлений в сфере компьютерной информации. Особенности личности компьютерного преступника.	2	2	-	2	2	-

8.	Основные направления и меры борьбы с преступлениями в сфере компьютерной информации в РФ.	1	1	2	1	1	2
		15	**15**	**6**	**15**	**15**	**6**

5.2. Лекционные занятия

Таблица 4

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	Основные законы и понятия современного информационного оборота.	1.Правовое понятие и сущность компьютерной информации. 2.Основные нормативно-правовые акты, регулирующие современный информационный оборот. 3.Понятийный аппарат, применяемый при исследовании преступлений в сфере компьютерной информации.
2.	Современная криминологическая оценка преступлений в сфере компьютерной информации.	1.Состояние, уровень, структура и динамика преступлений в сфере компьютерной информации. 2.Латентность преступлений в сфере компьютерной информации. 3. Понятие сетевого компьютерного преступления. Типология сетевых компьютерных преступлений. 4.Использование основных понятий, категорий, институтов, правовых статусов субъектов уголовных правоотношений в криминологической оценке преступлений в сфере компьютерной информации.
3.	Уголовно-правовая характеристика преступлений в сфере компьютерной информации по УК РФ.	1. Неправомерный доступ к компьютерной информации (ст. 272 УК). 2. Создание, использование и распространение вредоносных компьютерных программ (ст. 273 УК). 3. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей (ст. 274 УК). 4. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации (ст. 274.1 УК).
4.	Виды преступлений и опасных деяний в сфере обращения цифровой информации, нуждающихся в криминализации.	1. Мошенничество в сфере компьютерной информации. 2. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации. 3. Незаконный оборот специальных технических

		средств, предназначенных для нарушения систем защиты цифровой информации. 4. Приобретение или сбыт цифровой информации, заведомо добытой преступным путем. 5. Составы преступлений, содержащие квалифицирующий признак «с использованием информационно- телекоммуникационных сетей».
5.	Вопросы квалификации преступлений в сфере компьютерной информации.	1. Соотношение составов преступлений в сфере компьютерной информации со смежными и иными составами преступлений 2. Место совершения преступлений в сфере компьютерной информации. 3. Отдельные проблемные вопросы, связанные с моментом окончания преступлений в сфере компьютерной информации.
6.	Состояние и тенденции развития зарубежного и международного уголовного законодательства в сфере защиты компьютерной информации.	1. Правовые основы борьбы с преступлениями в сфере компьютерной информации в зарубежных странах. 2. Подходы различных государств к криминализации преступлений в сфере компьютерной информации. 3. Общая характеристика и виды преступлений в сфере компьютерной информации по уголовному законодательству зарубежных стран. 4. Сравнительно-правовой анализ отдельных преступлений в сфере компьютерной информации в зарубежном уголовном законодательстве 5. Международные соглашения в сфере борьбы с компьютерными преступлениями. Международная Конвенция по борьбе с киберпреступностью от 23 ноября 2001 г. Правовые основы борьбы с преступлениями в сфере компьютерной информации в странах СНГ.
7.	Причины и условия преступлений в сфере компьютерной информации. Особенности личности компьютерного преступника.	1. Причины и условия преступлений в сфере компьютерной информации. 2. Особенности личности преступника в сфере компьютерной информации. 3. Типология личности преступника в сфере компьютерной информации. 4. Особенности лиц, совершающих преступления в глобальных компьютерных сетях.
8.	Основные направления и меры борьбы с преступлениями в сфере компьютерной информации в РФ.	1. Основные направления профилактики преступлений в сфере компьютерной информации. 2. Правовое регулирование борьбы с преступлениями в сфере компьютерной информации. 3. Меры предупреждения преступлений в сфере компьютерной информации. 4. Виктимологическая профилактика преступлений в сфере компьютерной информации. 5. Система субъектов, осуществляющих борьбу с

		преступлениями в сфере компьютерной информации. 6. Особенности предупреждения преступлений в глобальных компьютерных сетях.

5.3. Лабораторный минимум не предусмотрен

5.4. Практические занятия (семинары)

Таблица 5

№ п/п	Наименование раздела дисциплины	Содержание раздела
1.	Основные законы и понятия современного информационного оборота.	Анализ нормативно-правовых актов.
2.	Современная криминологическая оценка преступлений в сфере компьютерной информации.	Решение кейс-задач с акцентом на уточнение норм законодательства.
3.	Уголовно-правовая характеристика преступлений в сфере компьютерной информации по УК РФ.	Написание эссе на определенную статью законодательства с полным анализом.
4.	Виды преступлений и опасных деяний в сфере обращения цифровой информации, нуждающихся в криминализации.	Обсуждение темы «Виды преступлений и опасных деяний в сфере обращения цифровой информации, нуждающихся в криминализации», обсуждение современных трудов.
5.	Вопросы квалификации преступлений в сфере компьютерной информации.	Решение кейс-задач по уголовной квалификации.
6.	Состояние и тенденции развития зарубежного и международного уголовного законодательства в сфере защиты компьютерной информации.	Обсуждение темы «Состояние и тенденции развития зарубежного и международного уголовного законодательства в сфере защиты компьютерной информации».
7.	Причины и условия преступлений в сфере компьютерной информации. Особенности личности компьютерного преступника.	Построение портрета преступника, обсуждение инструментов составления портрета преступника.
8.	Основные направления и меры борьбы с преступлениями в сфере компьютерной информации в РФ.	Обсуждение научных дискуссий и практики по теме «Основные направления и меры борьбы с преступлениями в сфере компьютерной информации в РФ»

6. Самостоятельная работа студентов по дисциплине

Самостоятельная работа студентов, направленная на углубление и закрепление знаний, заключается в:

- работе студентов с лекционным материалом, поиск и анализ литературы и электронных источников информации по заданной теме;
- изучение тем, вынесенных на самостоятельную проработку;
- изучение теоретического материала к практическим занятиям;
- написание реферата;
- подготовке к зачету.

6.1 Темы для самостоятельного изучения

1. Значение информации в жизни социума.
2. Научно-техническая революция и социальное развитие.
3. Правовое понятие и сущность компьютерной информации.
4. Понятийный аппарат, применяемый при исследовании преступлений в сфере компьютерной информации.
5. Понятие сетевого компьютерного преступления.
6. Типология сетевых компьютерных преступлений.
7. 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 (ст. 274.2 УК РФ).
8. Составы преступлений, содержащие квалифицирующий признак «с использованием информационно- телекоммуникационных сетей».
9. Отдельные проблемные вопросы, связанные с моментом окончания преступлений в сфере компьютерной информации.
10. Виктимологическая профилактика преступлений в сфере компьютерной информации.

6.2 Темы для 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. Будапешстская конвенция о киберпреступности.

24. Противодействие кибертерроризму и пропаганде экстремизма в сети Интернет.

25. Использование технологий искусственного интеллекта для совершения киберпреступлений.

6.3 Учебно-методическое обеспечение самостоятельной работы

Современные профессиональные базы данных:

1. http://elibrary.ru/ - Научная электронная библиотека
2. http://www.biblioclub.ru/ - Евразийский открытый институт
3. http://www.net.nns.ru - /Национальная электронная библиотека
4. http://www.rsl.ru/ - Российская государственная библиотека
5. http://www.runivers.ru - Электронная библиотека Руниверс 35
6. www.garant.ru – Справочная правовая система «Гарант»
7. www.consultant.ru – Справочная правовая система «Консультант Плюс»
8. www.supcourt.ru – Верховный суд Российской Федерации

7. Оценочные средства

7.1. 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.

Образец билета к зачету

Грозненский государственный нефтяной технический университет им.акад. М.Д. Миллионщикова
Институт ""
Группа "" Семестр "3"
Дисциплина "Киберправо"
Билет № 1

1. Цифровое право и примеры его реализации.
2. Принципы обработки персональных данных в сети Интернет.

Подпись преподавателя_____ Подпись заведующего кафедрой_____

7.2 Текущий контроль

Задание №1.

Студент заочного отделения Шатурин решил использовать компьютер из компьютерного класса университета для оформления контрольных и курсовых работ. Без разрешения деканата факультета он проник в класс и стал работать на компьютере. Из-за поверхностных знаний и навыков работы на компьютере произошли сбои в работе машины, что привело в дальнейшем к отключению модема — одного из элементов компьютерной системы.

Вопросы: подлежит ли уголовной ответственности Шатурин? Дайте анализ состава преступления, предусмотренного ст.274 УК РФ. Что понимается под информационно-телекоммуникационными сетями и оконечным оборудованием в смысле ст. 274 УК РФ? Какие виды оконечного оборудования возможны? Относится ли к оконечному оборудованию телефонный модем?

Задание №2.

Бережной заказал знакомому программисту Пятеркину написать программу, находящую и расширяющую бреши в защите персональных компьютеров и информационно-телекоммуникационных сетей. С ее помощью Бережной проник в сеть банка «Капитал» и уничтожил всю информацию о предоставлении ему кредита в размере 1,5 млн рублей.

Вопросы: По какой статье (части статьи) УК РФ следует квалифицировать действия Бережного. Раскрыть: Объект, Объективную сторону, Субъект, Субъективную сторону.

Задание №3.

Вы – начальник информационной службы в ЛПУ. У вас возникли подозрения, что сотрудник вашей организации позволил себе неправомерный доступ к охраняемой законом компьютерной информации, что повлекло уничтожение и блокирование информации. Внутренняя проверка факт неправомерного доступа подтвердила.

Вопросы: Какая статья уголовного кодекса подлежит применению? Какое наказание должен понести нарушитель?

Задание №4.

Руководитель отдела информационной безопасности организации установил, что один из пользователей корпоративной информационной системы создает и распространяет вредоносные программы внутри сети.

Вопросы: Какая статья уголовного кодекса подлежит применению? Какое наказание должен понести нарушитель?

Задание №5.

Гражданин П. проник в информационную базу государственного учреждения и скопировал интересующую его информацию с ограниченным доступом, о чем стало известно администраторам информационной системы. Через неделю ему пришла повестка в суд.

Вопросы: являются ли его действия противозаконными? С чем это связано? Какое наказание может ждать гражданина П. за совершенные им действия?

Задание №6.

Гражданин С. являясь администратором автоматизированной информационно-поисковой системы (АИПС), как инженер-программист регионального отдела информационного обеспечения, наделенный высшим уровнем доступа в Сеть, произвел незаконные уничтожение охраняемой законом служебной информации о совершении рядом лиц административных правонарушений и лишении их права управления транспортными средствами.

Вопрос: как следует квалифицировать содеянное С.

Задание №7.

К., находясь у себя дома, имея свободный доступ к сети Интернет, используя кабель для сети Интернет, ноутбук «DELL», осуществил соединение с сервером собственника информационных ресурсов «Филиал в г. Барнауле ЗАО «ЭР-Телеком Холдинг», предоставляющего услуги доступа к компьютерной сети Интернет, в сети Интернет зашел на электронный ресурс ООО «Мэйл.ру», после чего, незаконно используя учетную запись в виде логина «Iarantl972@mail.ru», принадлежащего А., ввел его в поле «Логин», а затем, воспользовавшись системой восстановления пароля через ключевое слово, в поле «секретный вопрос - больница», ввел слово «краевая», а в строке «пароль» ввел новый пароль «12345g». После чего, К., активировал клавишу «войти» и тем, самым совершил неправомерный доступ к электронному почтовому ящику «Iarantl972@mail.ru», принадлежащему А, что повлекло модификацию компьютерной информации на электронном почтовом ящике А. и сервере собственника информационных ресурсов ООО «Мэйл.ру», то есть, изменение ее содержания по сравнению с той информацией, которая первоначально была в распоряжении собственника информации и, поменяв пароль, заблокировал её, то есть создал условия невозможности использования информации собственником при её сохранности.

Вопрос: как следует квалифицировать содеянное К.

Задание №8.

Ш., Л., П., Щ. посредством сети Интернет приобрели у неустановленного лица техническое устройство «скиммер». Затем, используя подручные средства, совместными усилиями во фрагмент пластиковой трубы, обернутый фольгой, поместили видеокамеру с носителем информации и иные детали, изъятые из приобретенного для этой цели видеорегистратора, и привели их в рабочее состояние, тем самым изготовили самодельное техническое устройство «планка», предназначенное для установки на корпус банкомата, непосредственно над клавиатурой, с целью видеофиксации цифровых символов ПИН-кодов к

банковским картам граждан. После чего Ш., Л., П., Щ. совместно подыскали банкомат, конструктивно подходящий для установки технических устройств «скиммер» и «планка» и установили их. Во время работы указанных технических устройств, при самообслуживании в банкомате потерпевшие производили операции с личными банковскими картами. В результате этого Ш., Л., П., Щ с помощью технического устройства «скиммер» при прохождении через него банковских карт с их магнитных полос производилось считывание и копирование информации об индивидуальных цифровых свойствах банковских карт на встроенный носитель информации, а также с помощью технического устройства «планка» со скрытой видеокамерой и носителем информации была произведена видеофиксация последовательности набора данными клиентами на клавиатуре банкомата цифровых символов ПИН-кодов с сохранением указанных видеоданных. После чего установленные технические устройства демонтировались. Таким образом, Ш., Л., П., Щ осуществили неправомерный доступ к содержащейся на магнитных полосах информации об индивидуальных цифровых свойствах банковских карт, и, кроме того, в электронную память технических устройств, установленных подсудимыми, были скопированы сведения об индивидуальных цифровых свойствах банковских карт. Впоследствии Ш., Л., П., Щ преобразовывали данную информацию с помощью компьютера, делая ее пригодной для последующей записи на магнитные полосы новых пластиковых карт. Таким образом, были изготовлены дубликаты пластиковых карт. После чего Ш., сопоставив по времени и последовательности фиксации информацию, полученную с помощью технического устройства «скиммер», с информацией, полученной с помощью технического устройства «планка», определял цифровые символы ПИН-кода доступа к счету законного владельца каждой банковской карты и записывал их на отдельный лист в последовательности, раскладке дубликатов банковских карт. Впоследствии с помощью дубликатов банковских карт и полученных сведений о пин-кодах Ш., Л., П., Щ произвели операции по снятию денежных средств.

Вопросы: что понимается под копированием информации? Что будет инкриминировано Ш., Л., П., Щ.?

Задание №9.

Знакомый похитил расчетную пластиковую карту знакомого. Завладел денежной суммой в размере 5000 рублей. Следователь сказал, что будет предъявлено обвинение по ст. 272 УК РФ.

Вопрос: имеется ли указанный состав преступления?

Задание №10.

Сотрудник административных сетей организации в личных интересах «майнил» криптовалюту, не обновил защитную систему, допустил причинение вреда инфраструктуре.

Вопрос: квалифицируйте содеянное.

Задание №11.

Системный администратор учреждения при работе не использовал систему безопасности. В результате было осуществлено копирование информации с персональными данными сотрудников и личными контактами коммерческих партнеров, что причинило учреждению крупный ущерб. Уголовное дело было ошибочно возбуждено по ст. 272 УК РФ и передано в суд. Постановленный судебный приговор был отменен надзорной инстанцией, уголовное дело прекращено, по обстоятельствам истечения сроков привлечения к уголовной ответственности. Следственные и судебные органы не учли, что преступление совершил специальный субъект - законный пользователь.

Вопрос: по какой статье (части статьи) уголовного закона следовало квалифицировать деяние.

Задание №12.

Судом установлено, что с марта по апрель этого года студент К. с домашнего компьютера произвел ряд DDoS- атак (распределенных атак типа "отказ в обслуживании") на компьютерную информацию, хранящуюся на ресурсах сайтов ЗАО Банк "Тиньк", ЗАО "Лаборатория Каспера", ОАО "Промвязьбанк" и ЗАО "Издательский дом "Комсомольская неправда".

В итоге была блокирована работа этих сайтов, в том числе личных кабинетов пользователей интернет-банка, мобильных банка и кошелька, систем СМС-информирования, POS-терминалов в интернете, продажа продуктов на сайтах, а также системы авторизации и офисного интернета – Wi-Fi.24 марта студент К. в одной из соцсетей потребовал от владельца банка "ТКС" $1000 за прекращение DDoS- атаки. Когда же банкир отказался платить и пригрозил хакеру уголовной ответственностью, тот увеличил требуемую сумму до $3000.

Вскоре Кузьмин был задержан сотрудниками полиции. Общий ущерб, причиненный им правообладателям, превысил 11 млн руб.

Вопрос: По каким статьям уголовного закона Кузьмин будет признан судом виновным?

Задание №13.

Солдатова в начале декабря 2016 года в вечернее время находилась в квартире знакомой Мещеряковой с малознакомой Рахмановой. Рахманова, ложась спать, разрешила ей пользоваться своим сотовым телефоном. Увидев, что на телефон Рахмановой пришло смс - сообщение о поступлении денег на карту она решила похитить данные денежные средства со счета карты. С телефона Рахмановой набрала команду перевод с карты на карту, указав номер карты, оформленной на ее имя, сумму перевода. Дважды она перевела по 4000 рублей на свою

карту, приходящие смс- сообщения о списании денежных средств она удаляла. После перевода денег она ушла, из квартиры, сняла со своей карты денежные средства в сумме 8000 рублей, которые потратила на личные нужды.

Вопрос: Какое преступление совершила Солдатова?

Задание №14.

Сотрудник организации, по специальности программист, разработал антивирусную программу. С целью продолжения работы (на период отпуска) забрал копию на флеш-карте домой. Его ребенок без разрешения взял носитель информации, запустил вирус в сеть на уроке информатики. Из-за этого был причинен вред электронной системе образовательного учреждения.

Вопрос: Какая ответственность грозит программисту?

Задание №15.

Иванов, работая в организации связи, подсмотрел данные для входа в специальную систему, ознакомился с детализацией звонков невесты.

Вопросы: усматривается ли в действиях Иванова состав преступления?

7.3. Описание показателей и критериев оценивания компетенций на различных этапах и формирования, описание шкалы оценивания.

Таблица 6

Планируемые результаты освоения компетенции	**Критерии оценивания результатов обучения**				**Наименование оценочного средства**
	Менее 41 баллов (неудовлетворительно)	**41-60 баллов (удовлетворительно)**	**61-80 баллов (хорошо)**	**81-100 баллов (отлично)**	
ПК-2. Способен квалифицированно применять нормативные правовые акты в конкретных сферах юридической деятельности, реализовывать нормы материального и процессуального права в профессиональной деятельности					
Знать: нормы материального и процессуального права.	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные систематические знания	опрос, практические задания, темы рефератов, темы докладов, тестовые задания.
Уметь: реализовать нормы материального и процессуального права в профессиональной деятельности.	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные знания	опрос, практические задания, темы рефератов, темы докладов, тестовые задания.
Владеть: навыками работы с правовыми актами, на основе их анализа принимает решения о реализации норм материального и процессуального права в профессиональной деятельности.	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	опрос, практические задания, темы рефератов, темы докладов, тестовые задания.
ПК-5. Способен защищать права и законные интересы субъектов права					

Знать: законодательство в сфере информационных технологий, киберпреступности, формы и способы защиты нарушенных прав и особенности их применения.	Фрагментарные знания	Неполные знания	Сформированные, но содержащие отдельные пробелы знания	Сформированные, систематические знания	опрос, практические задания, темы рефератов, темы
Уметь: применять нормы закона в области информационной безопасности.	Частичные умения	Неполные умения	Умения полные, допускаются небольшие ошибки	Сформированные умения	опрос, практические задания, темы рефератов, темы докладов, тестовые задания.
Владеть: навыками анализа и применения нормативных правовых актов в сфере информационной безопасности.	Частичное владение навыками	Несистематическое применение навыков	В систематическом применении навыков допускаются пробелы	Успешное и систематическое применение навыков	опрос, практические задания, темы рефератов, темы докладов, тестовые задания.

8. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья

Для осуществления процедур текущего контроля успеваемости и промежуточной аттестации обучающихся созданы фонды оценочных средств, адаптированные для инвалидов и лиц с ограниченными возможностями здоровья и позволяющие оценить достижение ими запланированных в основной образовательной программе результатов обучения и уровень сформированности всех компетенций, заявленных в образовательной программе. Форма проведения текущей аттестации для студентов-инвалидов устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При тестировании для слабовидящих студентов используются фонды оценочных средств с укрупненным шрифтом. На экзамен приглашается сопровождающий, который обеспечивает техническое сопровождение студенту. При необходимости студенту-инвалиду предоставляется дополнительное время для подготовки ответа на экзамене (или зачете). Обучающиеся с ограниченными возможностями здоровья, и обучающиеся инвалиды обеспечиваются печатными и электронными образовательными ресурсами (программы, учебные пособия для самостоятельной работы и т.д.) в формах, адаптированных к ограничениям их здоровья и восприятия информации:

1) для инвалидов и лиц с ограниченными возможностями здоровья по зрению:

- для слепых: задания для выполнения на семинарах и практических занятиях оформляются рельефно-точечным шрифтом Брайля или в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением для слепых, либо зачитываются ассистентом; письменные задания выполняются на бумаге рельефно-точечным шрифтом Брайля или на компьютере со специализированным программным обеспечением для слепых либо надиктовываются ассистенту; обучающимся для выполнения задания при необходимости предоставляется комплект письменных принадлежностей и бумага для письма рельефно-точечным шрифтом Брайля, компьютер со специализированным программным обеспечением для слепых;

- для слабовидящих: обеспечивается индивидуальное равномерное освещение не менее 300 люкс; обучающимся для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств; задания для выполнения заданий оформляются увеличенным шрифтом;

2) для инвалидов и лиц с ограниченными возможностями здоровья по слуху:

- для глухих и слабослышащих: обеспечивается наличие звукоусиливающей аппаратуры коллективного пользования, при необходимости обучающимся предоставляется звукоусиливающая аппаратура индивидуального пользования; предоставляются услуги

сурдопереводчика;

- для слепоглухих допускается присутствие ассистента, оказывающего услуги тифлосурдопереводчика (помимо требований, выполняемых соответственно для слепых и глухих);

3) для лиц с тяжелыми нарушениями речи, глухих, слабослышащих лекции и семинары, проводимые в устной форме, проводятся в письменной форме;

4) для инвалидов и лиц с ограниченными возможностями здоровья, имеющих нарушения опорно-двигательного аппарата:

- для лиц с нарушениями опорно-двигательного аппарата, нарушениями двигательных функций верхних конечностей или отсутствием верхних конечностей: письменные задания выполняются на компьютере со специализированным программным обеспечением или надиктовываются ассистенту; выполнение заданий (тестов, контрольных работ), проводимые в письменной форме, проводятся в устной форме путем опроса, беседы с обучающимся.

9. Учебно-методическое и информационное обеспечение дисциплины

Основная литература:

1. Степанов – Егиянц В.Г. Ответственность за преступления против компьютерной информации по уголовному законодательству Российской Федерации: монография - Москва: Статут, 2016.

2. Корабельников, С. М. Преступления в сфере информационных отношений: учебное пособие - Москва: Всероссийский государственный университет юстиции (РПА Минюста России), 2015.

Дополнительная литература:

3. Борисов С. Преступления в сфере компьютерной информации: монография - Москва: Лаборатория книги, 2010.

4. Милашевская Е. С. Уголовная ответственность за преступления в сфере компьютерной информации: монография - Москва: Лаборатория книги, 2012.

10. Материально-техническое обеспечение дисциплины

Помещения для всех видов работ, предусмотренных учебным планом, укомплектованы необходимой специализированной учебной мебелью и техническими средствами обучения:

- столы, стулья;
- персональный компьютер / ноутбук;
- проектор;
- экран / интерактивная доска.

Составитель:

к. ю. н., зав. кафедры «Юриспруденция»  М.Р. Богатырев

Согласовано:

и.о. Зав. выпускающей кафедрой

«Юриспруденция»  М.Р. Богатырев

Директор ДУМР  М.А. Магомаева

Приложение

Методические указания по освоению дисциплины «Киберпреступность и информационная безопасность»

1. Методические указания для обучающихся по планированию и организации времени, необходимого для освоения дисциплины.

Изучение рекомендуется начать с ознакомления с рабочей программой дисциплины, ее структурой и содержанием разделов (модулей), фондом оценочных средств, ознакомиться с учебно-методическим и информационным обеспечением дисциплины.

Дисциплина «Киберпреступность и информационная безопасность» состоит из 8 связанных между собою тем, обеспечивающих последовательное изучение материала.

Обучение по дисциплине «Киберпреступность и информационная безопасность» осуществляется в следующих формах:

1. Аудиторные занятия (лекции, практические занятия).

2. Самостоятельная работа студента (подготовка к лекциям, практическим занятиям, тестам/рефератам/докладам/, и иным формам письменных работ, выполнение анализа кейсов, индивидуальная консультация с преподавателем).

Описание последовательности действий обучающегося:

При изучении курса следует внимательно слушать и конспектировать материал, излагаемый на аудиторных занятиях. Для его понимания и качественного усвоения рекомендуется следующая последовательность действий:

1. После окончания учебных занятий для закрепления материала просмотреть и обдумать текст лекции, прослушанной сегодня, разобрать рассмотренные примеры (10 – 15 минут).

2. При подготовке к лекции следующего дня повторить текст предыдущей лекции, подумать о том, какая может быть следующая тема (10 - 15 минут).

3. В течение недели выбрать время для работы с литературой в библиотеке (по 1часу).

4. При подготовке к практическому/ семинарскому занятию повторить основные понятия по теме, изучить примеры. Решая конкретную ситуацию, - предварительно понять, какой теоретический материал нужно использовать. Наметить план решения, попробовать на его основе решить 1 - 2 практические ситуации (лаб. работы).

2. Методические указания по работе обучающихся во время проведения лекций.

Лекции дают обучающимся систематизированные знания по дисциплине, концентрируют их внимание на наиболее сложных и важных вопросах. Лекции обычно

излагаются в традиционном или в проблемном стиле. Для студентов в большинстве случаев в проблемном стиле. Проблемный стиль позволяет стимулировать активную познавательную деятельность обучающихся и их интерес к дисциплине, формировать творческое мышление, активизировать внимание обучающихся путем постановки проблемных вопросов, поощрять дискуссию.

Во время лекционных занятий рекомендуется вести конспектирование учебного материала, обращать внимание на формулировки и категории, раскрывающие суть того или иного явления, или процессов, выводы и практические рекомендации.

Конспект лекции лучше подразделять на пункты, соблюдая красную строку. Этому в большой степени будут способствовать вопросы плана лекции, предложенные преподавателям. Следует обращать внимание на акценты, выводы, которые делает преподаватель, отмечая наиболее важные моменты в лекционном материале замечаниями

«важно», «хорошо запомнить» и т.п. Можно делать это и с помощью разноцветных маркеров или ручек, подчеркивая термины и определения.

Целесообразно разработать собственную систему сокращений, аббревиатур и символов. Однако при дальнейшей работе с конспектом символы лучше заменить обычными словами для быстрого зрительного восприятия текста.

Работая над конспектом лекций, необходимо использовать не только основную литературу, но и ту литературу, которую дополнительно рекомендовал преподаватель. Именно такая серьезная, кропотливая работа с лекционным материалом позволит глубоко овладеть теоретическим материалом.

Тематика лекций дается в рабочей программе дисциплины.

3. Методические указания обучающимся по подготовке к практическим занятиям.

На практических занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный материал по тематике семинарских занятий.

Студенту рекомендуется следующая схема подготовки к семинарскому занятию:

1. Ознакомление с планом практических занятий, который отражает содержание предложенной темы;

2. Проработать конспект лекций;

3. Прочитать основную и дополнительную литературу.

В процессе подготовки к практическим занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы. При всей полноте конспектирования лекции в ней невозможно изложить весь материал из-за лимита аудиторных

часов. Поэтому самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у студентов отношение к конкретной проблеме. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса;

4. Ответить на вопросы плана практических занятиях;

5. Выполнить домашнее задание;

6. Проработать тестовые задания и задачи;

7. При затруднениях сформулировать вопросы к преподавателю.

Результат такой работы должен проявиться в способности студента свободно ответить на теоретические вопросы, выступать и участвовать в коллективном обсуждении вопросов изучаемой темы, правильно выполнять задания на практических занятиях, которые даются в фонде оценочных средств дисциплины.

4. Методические указания обучающимся по организации самостоятельной работы.

Цель организации самостоятельной работы по дисциплине «Киберпреступность и информационная безопасность» — это углубление и расширение знаний в области фундаментальных исследований; формирование навыка и интереса к самостоятельной познавательной деятельности.

Самостоятельная работа обучающихся является важнейшим видом освоения содержания дисциплины, подготовки к практическим занятиям и к контрольной работе. Сюда же относятся и самостоятельное углубленное изучение тем дисциплины. Самостоятельная работа представляет собой постоянно действующую систему, основу образовательного процесса и носит исследовательский характер, что послужит в будущем основанием для написания выпускной квалификационной работы, практического применения полученных знаний.

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению, с учетом потребностей и возможностей личности.

Правильная организация самостоятельных учебных занятий, их систематичность, целесообразное планирование рабочего времени позволяет студентам развивать умения и навыки в усвоении и систематизации приобретаемых знаний, обеспечивать высокий уровень успеваемости в период обучения, получить навыки повышения профессионального уровня.

Подготовка к практическим занятиям включает, кроме проработки конспекта и презентации лекции, поиск литературы (по рекомендованным спискам и самостоятельно), подготовку заготовок для выступлений по вопросам, выносимым для обсуждения по конкретной теме. Такие заготовки могут включать цитаты, факты, сопоставление различных позиций, собственные мысли. Если проблема заинтересовала обучающегося, он может подготовить реферат и выступить с ним на практическом занятии. При подготовке к контрольной работе обучающийся должен повторять пройденный материал в строгом соответствии с учебной программой, используя конспект лекций и литературу, рекомендованную преподавателем. При необходимости можно обратиться за консультацией и методической помощью к преподавателю.

Самостоятельная работа реализуется:

– непосредственно в процессе аудиторных занятий - на лекциях, практических занятиях;

– в контакте с преподавателем вне рамок расписания - на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.

– в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Виды СРС и критерии оценок

(по балльно-рейтинговой системе ГГНТУ)

1. Реферат

2. Доклад

3. Участие в мероприятиях

Темы для самостоятельной работы прописаны в рабочей программе дисциплины. Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.