Рабочая программа дисциплины (модуля)*

Проблемы противодействия информационной преступности

Направление подготовки (специальность)

40.04.01 Юриспруденция

Направленность (профиль)

Юрист по уголовным делам

Присваиваемая квалификация (степень)

Магистр

Форма обучения

заочная

Год(ы) набора 2026

*Рабочая программа дисциплины (модуля) адаптирована для инклюзивного обучения инвалидов и лиц с ограниченными возможностями здоровья

Челябинск 2026 г.

Содержание

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель освоения дисциплины – получение обучающимися в систематизированном виде знаний в области правового и организационного обеспечения информационной безопасности и навыков противодействия правонарушениям против информационной безопасности.

Результаты обучения по дисциплине направлены на достижение индикаторов:

ПК-1.1. Применяет нормы уголовного законодательства при производстве по уголовным делам;

ПК-1.2. Применяет нормативные акты других отраслей права при производстве по уголовным делам.

ПК-2.1. Оказывает консультационные услуги по уголовным делам.

ПК-2.2. Оказывает услуги представительства отдельных участников уголовного процесса.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.В.ДВ.02.01

2.1 Требования к предварительной подготовке обучающегося:

Актуальные проблемы уголовного права

Проблемы квалификации преступлений (научный семинар)

2.2 Дисциплины и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:

Подготовка к процедуре защиты и защита выпускной квалификационной работы

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

ПК-1: Способен применять уголовное законодательство, а также другие виды нормативных актов при производстве по уголовным делам

Знать:

Для достижения ПК-1.1. знать: предусмотренные законом средства защиты прав и свобод человека и гражданина, охраняемых законом интересов общества и государства; методы выявления и устранения нарушений закона в информационной сфере;
Для достижения ПК-1.2. знать: предусмотренные законом средства защиты прав и свобод человека и гражданина, интересов общества и государства в информационной сфере; методику применения мер к устранению выявленных нарушений в информационной сфере.

Уметь:

Для достижения ПК-1.1. уметь: применять предусмотренные законом средства защиты прав и свобод человека и гражданина, охраняемых законом интересов общества и государства; методы выявления и устранения нарушений закона в информационной сфере;
Для достижения ПК-1.2. уметь: применять предусмотренные законом средства защиты прав и свобод человека и гражданина, интересов общества и государства в информационной сфере; использовать методику применения мер к устранению выявленных нарушений в информационной сфере.

Владеть:

Для достижения ПК-1.1. владеть: навыками применения предусмотренных законом средств защиты прав и свобод человека и гражданина, охраняемых законом интересов общества и государства; методов выявления и устранения нарушений закона в информационной сфере;
Для достижения ПК-1.2. владеть: навыками применения предусмотренных законом средств защиты прав и свобод человека и гражданина, интересов общества и государства в информационной сфере; использования методики применения мер к устранению выявленных нарушений в информационной сфере.

ПК-2: Способен оказывать консультационные услуги по уголовным делам и услуги представительства отдельных участников уголовного процесса

Знать:

Для достижения ПК-2.1. знать: методику толкования уголовно-правовых норм при оказании консультационных услуг по уголовным делам в информационной сфере

Уметь:

Для достижения ПК-2.1. уметь: применять методику толкования уголовно-правовых норм при оказании

консультационных услуг по уголовным делам в информационной сфере

Владеть:

Для достижения ПК-2.1. владеть: методикой толкования уголовно-правовых норм при оказании консультационных услуг по уголовным делам в информационной сфере

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	предусмотренные законом средства защиты прав и свобод человека и гражданина, охраняемых законом интересов общества и государства; методы выявления и устранения нарушений закона в информационной сфере;
3.1.2	предусмотренные законом средства защиты прав и свобод человека и гражданина, интересов общества и государства в информационной сфере;
3.1.3	методику применения мер к устранению выявленных нарушений в информационной сфере;
3.1.4	методику толкования уголовно-правовых норм при оказании консультационных услуг по уголовным делам в информационной сфере;
3.1.5	понятие, виды и причины возникновения пробелов в уголовном праве, основные способы их восполнения; понятие, виды, причины возникновения коллизий норм уголовного права, основные способы и правила их разрешения;
3.1.6	методику анализа проблемных ситуаций в сфере уголовного права с целью формирования правил его применения; методику аргументации собственных суждений и оценок при применении уголовного законодательства в информационной сфере.
3.2	**Уметь:**
3.2.1	применять предусмотренные законом средства защиты прав и свобод человека и гражданина, охраняемых законом интересов общества и государства; методы выявления и устранения нарушений закона в информационной сфере;
3.2.2	применять предусмотренные законом средства защиты прав и свобод человека и гражданина, интересов общества и государства в информационной сфере;
3.2.3	использовать методику применения мер к устранению выявленных нарушений в информационной сфере;
3.2.4	выявлять причины возникновения пробелов в уголовном праве, основные способы их восполнения; причины возникновения коллизий норм уголовного применять методику анализа проблемных ситуаций по уголовным делам в информационной сфере; методику аргументации собственных суждений и оценок при применении уголовного законодательства в информационной сфере.
3.3	**Владеть:**
3.3.1	применения предусмотренных законом средств защиты прав и свобод человека и гражданина, охраняемых законом интересов общества и государства; методов выявления и устранения нарушений закона в информационной сфере;
3.3.2	применения предусмотренных законом средств защиты прав и свобод человека и гражданина, интересов общества и государства в информационной сфере;
3.3.3	использования методики применения мер к устранению выявленных нарушений в информационной сфере;
3.3.4	применения методики толкования уголовно-правовых норм при оказании консультационных услуг по уголовным делам в информационной сфере;
3.3.5	выявления причин возникновения пробелов в уголовном праве, основных способов их восполнения; причин возникновения коллизий норм уголовного права, основных способов и правил их разрешения;
3.3.6	применения методики анализа проблемных ситуаций по уголовным делам в информационной сфере; методики аргументации собственных суждений и оценок при применении уголовного законодательства в информационной сфере.

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)

Общая трудоемкость	**3 ЗЕТ**
Часов по учебному плану : 108 в том числе : аудиторные занятия : 8 самостоятельная работа : 95,1 часов на контроль : 4 контактная работа: 8,9 ИКР: 0,9	Виды контроля на курсах: зачеты 2

5. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Литература
	Раздел 1. Основы теории обеспечения информационной безопасности			
1.1	Информационная безопасность в информационном обществе /Лек/	2	1	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
1.2	Информационная безопасность в системе обеспечения национальной безопасности /Ср/	2	8	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
1.3	Основные угрозы информационной безопасности /Пр/	2	1	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
1.4	Информация как объект обеспечения безопасности /Ср/	2	6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
	Раздел 2. Правовое обеспечение информационной безопасности			
2.1	Правовые режимы обеспечения информации ограниченного доступа /Лек/	2	1	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
2.2	Правовые проблемы обеспечения безопасности в сети Интернет /Лек/	2	2	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
2.3	Правовые проблемы обеспечения безопасности в сети Интернет /Ср/	2	2	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
2.4	Правовые средства обеспечения информационной безопасности /Ср/	2	10	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
2.5	Правовые режимы обеспечения информации ограниченного доступа /Ср/	2	2	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
2.6	Правовые проблемы обеспечения безопасности в сети Интернет /Ср/	2	10	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
2.7	Защита детей от информации, причиняющей вред их здоровью и развитию /Лек/	2	2	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
2.8	Защита детей от информации, причиняющей вред их здоровью и развитию /Ср/	2	6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
	Раздел 3. Юридическая ответственность за правонарушения в сфере обеспечения информационной безопасности			

3.1	Дисциплинарная ответственность за информационные правонарушения /Ср/	2	1	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
3.2	Административные правонарушения в области связи и информации /Ср/	2	6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
3.3	Уголовная ответственность за преступления в сфере информации /Ср/	2	6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
3.4	Дисциплинарная ответственность за информационные правонарушения /Ср/	2	4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
	Раздел 4. Криминологическое обеспечение информационной безопасности			
4.1	Понятие, свойства и типология преступности против информационной безопасности /Ср/	2	6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
4.2	Состояние, структура и динамика преступности против общественной безопасности /Ср/	2	4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
4.3	Виктимологические проблемы обеспечения информационной безопасности /Ср/	2	6	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
4.4	Личность «информационного» преступника /Ср/	2	4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
4.5	Особенности детерминант преступности против информационной безопасности /Ср/	2	4	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
4.6	Меры предупреждения и борьбы с преступностью против информационной безопасности /Пр/	2	1	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
4.7	Меры предупреждения и борьбы с преступностью против информационной безопасности /Ср/	2	10,1	Л1.1 Л1.2Л2.1 Л2.2 Э1 Э2
4.8	Индивидуальные консультации, текущий контроль /ИКР/	2	0,9	Л1.1 Л1.2 Э1 Э2

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Для текущей аттестации - кейс-задачи, устный опрос, тестирование.
Для промежуточной аттестации - собеседование, кейс-задачи.

6.2. Типовые контрольные задания и иные материалы для текущей аттестации

Примерные кейс-задачи к практическим занятиям
1. ГУВД Московской области было возбуждено уголовное дело по факту совершения неправомерного доступа к охраняемой законом компьютерной информации в кассовых аппаратах одного из индивидуальных предпринимателей г. Павловский Посад Лебедева. Следствие квалифицировало действия Лебедева по ч. 2 ст. 272 УК РФ, т.е. как такое изменение информации в контрольно-кассовых аппаратах, при котором записанная в них сумма выручки за смену искусственно занижалась. Информация, содержащаяся в контрольно-кассовых аппаратах, признана следствием разновидностью компьютерной информации. Адвокат Лебедева настаивал на изменении квалификации.
Дайте юридическую оценку содеянному. Что следует понимать под компьютерной информацией?
2. Петров использовал доработанный мобильный телефон – «сканер», который позволял производить звонки за чужой счет. Всего в течение шести месяцев Петров таким образом «израсходовал» 15 тыс. руб. Можно ли считать информацию, содержащуюся в мобильном телефоне, компьютерной информацией? Как соотносятся компьютерная

информация и коммерческая тайна? Квалифицируйте содеянное Петровым.
3. Программист Мохов был признан судом виновным в деяниях, предусмотренных ч. 3 ст. 273 и ч. 1 ст. 165 УК РФ. С ноября по апрель Мохов рассылал клиентам пяти городских интернет-провайдеров «троянские» программы и получал логины с паролями, которыми пользовался для доступа в Интернет. Всего было доказано наличие 12 подобных эпизодов, в течение которых Мохов пользовался услугами Интернета без оплаты.
Правильно ли суд квалифицировал содеянное? В каких случаях возможна квалификация по совокупности деяний, предусмотренных ст. 272–274 УК РФ с иными составами преступлений? Что следует понимать под тяжкими последствиями применительно к составу преступления, предусмотренного ст. 273 УК РФ?
4. Панченко и Будин работали в компьютерной фирме, распространяли «троянские» программы и получали доступ к паролям пользователей компьютеров. Следствие квалифицировало распространение вирусных программ по ч. 1 ст. 273 УК РФ, а доступ к чужим паролям по ч. 1. ст. 272 УК РФ.
Дайте анализ объективных и субъективных признаков данных составов преступлений. Решите вопрос о квалификации содеянного.

Вопросы для устного опроса:
1. Обеспечение информационной безопасности
2. Правовое обеспечение информационной безопасности
3. Организационное обеспечение информационной безопасности
4. Информационное общество и обеспечение информационной безопасности
5. Информационное противоборство и обеспечение информационной безопасности
6. Информационно-техническое противоборство
7. Идеологическое противоборство
8. Международное сотрудничество в обеспечение информационной безопасности
9. Национальная безопасность Российской Федерации
10. Содержание национальных интересов РФ в информационной сфере
11. Принципы обеспечения информационной безопасности
12. Информационная инфраструктура
13. Угрозы безопасности информационно-коммуникационной инфраструктуры
14. Основные правовые средства противодействия угрозам
15. Основные виды информации как объекты обеспечения безопасности
16. Основные угрозы безопасности информации
17. Международно-правовые акты в области обеспечения информационной безопасности
18. Зарубежный опыт обеспечения информационной безопасности
19. Ограничение доступа к информации в целях защиты интересов личности, общества и государства
20. Правовые режимы тайн
21. Правовой режим защиты государственной тайны
22. Правовой режим коммерческой тайны
23. Правовой режим обеспечения безопасности персональных данных
24. Актуальные вопросы режима служебной тайны
25. Противодействие экстремисткой деятельности в информационной сфере
26. Защита детей от информации, причиняющей вред их здоровью и развитию
27. Правовые проблемы обеспечения информационной безопасности в сети Интернет
28. Неправомерный доступ к компьютерной информации
29. Создание, использование и распространение вредоносных компьютерных программ
30. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
31. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации
32. Преступления, совершаемые с использованием компьютерных технологий
33. Понятие, свойства и типология преступности против информационной безопасности
34. Состояние, структура и динамика преступности против общественной безопасности
35. Виктимологические проблемы обеспечения информационной безопасности
36. Личность «информационного» преступника
37. Особенности детерминант преступности против информационной безопасности
38. Меры предупреждения и борьбы с преступностью против информационной безопасности
39. Государственное управление в информационной сфере
40. Система и полномочия органов государственной власти, обеспечивающих право доступа к информации
41. Система и компетенция органов, обеспечивающих охрану государственной тайны.
42. Компетенция органов государственной власти, по обеспечению правового режима конфиденциальной информации
43. Информационное государство

44. Административные правонарушения в области связи и информации
45. Нарушение владельцем аудиовизуального сервиса установленного порядка распространения среди детей информации, причиняющей вред их здоровью и (или) развитию
46. Распространение владельцем аудиовизуального сервиса информации, содержащей публичные призывы к осуществлению террористической деятельности, материалов, публично оправдывающих терроризм, или других материалов, призывающих к осуществлению экстремистской деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности
47. Нарушение порядка изготовления или распространения продукции средства массовой информации
48. Нарушение правил защиты информации
49. Незаконная деятельность в области защиты информации
50. Разглашение информации с ограниченным доступом
51. Злоупотребление свободой массовой информации
52. Воспрепятствование распространению продукции средства массовой информации
53. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений
54. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации
55. Отказ в предоставлении гражданину информации
56. Воспрепятствование законной профессиональной деятельности журналистов
57. Разглашение государственной тайны
58. Незаконное получение сведений, составляющих государственную тайну
59. Утрата документов, содержащих государственную тайну
60. Неправомерное использование инсайдерской информации
61. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну
62. Осуществление деятельности на территории Российской Федерации иностранной или международной неправительственной организации, в отношении которой принято решение о признании нежелательной на территории Российской Федерации ее деятельности

Примерные тестовые задания по дисциплине
1. Под информационной безопасностью понимается…
А) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре.
Б) программный продукт и базы данных должны быть защищены по нескольким направ¬лениям от воздействия
В) нет правильного ответа

2. Защита информации – это..
А) комплекс мероприятий, направленных на обеспечение информационной безопасности.
Б) процесс разработки структуры базы данных в соответствии с требованиями пользователей
В) небольшая программа для выполнения определенной задачи

3. От чего зависит информационная безопасность?
А) от компьютеров
Б) от поддерживающей инфраструктуры
В) от информации

4. Основные составляющие информационной безопасности:
А) целостность
Б) достоверность
В) конфиденциальность

5. Доступность – это…
А) возможность за приемлемое время получить требуемую информационную услугу.
Б) логическая независимость
В) нет правильного ответа

6. Целостность – это..
А) целостность информации
Б) непротиворечивость информации
В) защищенность от разрушения

7. Конфиденциальность – это..
А) защита от несанкционированного доступа к информации
Б) программ и программных комплексов, обеспечивающих технологию разработки, отладки и внедрения создаваемых программных продуктов
В) описание процедур

8. Для чего создаются информационные системы?
А) получения определенных информационных услуг
Б) обработки информации
В) все ответы правильные

9. Целостность можно подразделить:
А) статическую
Б) динамичную
В) структурную

10. Где применяются средства контроля динамической целостности?
А) анализе потока финансовых сообщений
Б) обработке данных
В) при выявлении кражи, дублирования отдельных сообщений

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Примерные вопросы для собеседования
1. Обеспечение информационной безопасности
2. Правовое обеспечение информационной безопасности
3. Организационное обеспечение информационной безопасности
4. Информационное общество и обеспечение информационной безопасности
5. Информационное противоборство и обеспечение информационной безопасности
6. Информационно-техническое противоборство
7. Идеологическое противоборство
8. Международное сотрудничество в обеспечение информационной безопасности
9. Национальная безопасность Российской Федерации
10. Содержание национальных интересов РФ в информационной сфере
11. Принципы обеспечения информационной безопасности
12. Информационная инфраструктура
13. Угрозы безопасности информационно-коммуникационной инфраструктуры
14. Основные правовые средства противодействия угрозам
15. Основные виды информации как объекты обеспечения безопасности
16. Основные угрозы безопасности информации
17. Международно-правовые акты в области обеспечения информационной безопасности
18. Зарубежный опыт обеспечения информационной безопасности
19. Ограничение доступа к информации в целях защиты интересов личности, общества и государства
20. Правовые режимы тайн
21. Правовой режим защиты государственной тайны
22. Правовой режим коммерческой тайны
23. Правовой режим обеспечения безопасности персональных данных
24. Актуальные вопросы режима служебной тайны
25. Противодействие экстремисткой деятельности в информационной сфере
26. Защита детей от информации, причиняющей вред их здоровью и развитию
27. Правовые проблемы обеспечения информационной безопасности в сети Интернет
28. Неправомерный доступ к компьютерной информации
29. Создание, использование и распространение вредоносных компьютерных программ
30. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной информации и информационно-телекоммуникационных сетей
31. Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации
32. Преступления, совершаемые с использованием компьютерных технологий
33. Понятие, свойства и типология преступности против информационной безопасности
34. Состояние, структура и динамика преступности против общественной безопасности

35. Виктимологические проблемы обеспечения информационной безопасности
36. Личность «информационного» преступника
37. Особенности детерминант преступности против информационной безопасности
38. Меры предупреждения и борьбы с преступностью против информационной безопасности
39. Государственное управление в информационной сфере
40. Система и полномочия органов государственной власти, обеспечивающих право доступа к информации
41. Система и компетенция органов, обеспечивающих охрану государственной тайны.
42. Компетенция органов государственной власти, по обеспечению правового режима конфиденциальной информации
43. Информационное государство
44. Административные правонарушения в области связи и информации
45. Нарушение владельцем аудиовизуального сервиса установленного порядка распространения среди детей информации, причиняющей вред их здоровью и (или) развитию
46. Распространение владельцем аудиовизуального сервиса информации, содержащей публичные призывы к осуществлению террористической деятельности, материалов, публично оправдывающих терроризм, или других материалов, призывающих к осуществлению экстремистской деятельности либо обосновывающих или оправдывающих необходимость осуществления такой деятельности
47. Нарушение порядка изготовления или распространения продукции средства массовой информации
48. Нарушение правил защиты информации
49. Незаконная деятельность в области защиты информации
50. Разглашение информации с ограниченным доступом
51. Злоупотребление свободой массовой информации
52. Воспрепятствование распространению продукции средства массовой информации
53. Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений
54. Незаконный оборот специальных технических средств, предназначенных для негласного получения информации
55. Отказ в предоставлении гражданину информации
56. Воспрепятствование законной профессиональной деятельности журналистов
57. Разглашение государственной тайны
58. Незаконное получение сведений, составляющих государственную тайну
59. Утрата документов, содержащих государственную тайну
60. Неправомерное использование инсайдерской информации
61. Незаконные получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну
62. Осуществление деятельности на территории Российской Федерации иностранной или международной неправительственной организации, в отношении которой принято решение о признании нежелательной на территории Российской Федерации ее деятельности

Примерные кейс-задачи для промежуточной аттестации

1. Аспирант университета Хохлов 23 лет занимался исследовательской работой по компьютерной «вирусологии». Целью работы было выяснение масштаба глобальной сетевой инфраструктуры. В результате ошибки в механизме размножения вирусы, так называемые сетевые черви, проникли в университетскую компьютерную сеть и уничтожили информацию, содержащуюся в компьютерах факультетов и подразделений. В результате этого были полностью уничтожены списки сотрудников университета, расчеты бухгалтерии по зарплате, повреждены материалы научно-исследовательской работы, в том числе «пропали» две кандидатские и одна докторская диссертации.
Решите вопрос о правомерности действий Хохлова.
2. Инженер одного из оборонных заводов Григорьев работал с документами, содержащими сведения, относящиеся к государственной тайне (сведения особой важности). Однажды он рассказал о данных документах жене, чтобы подчеркнуть важность своей работы, так как жена упрекала его в том, что он задерживается на работе и мало времени уделяет семье. Через несколько дней, находясь в гостях у своей подруги Павловой, жена Григорьева похвалилась важной работой мужа, сообщив, что он якобы работает над новым видом оружия. Павлова рассказала об этом своему приятелю Бену Треверсу, сотруднику иностранной разведки. В результате этого деятельностью данного оборонного завода стала усиленно интересоваться спецслужба иностранного государства. Дайте оценку ситуации
3. Работник иностранного посольства в г. Москве, технический секретарь Джонсон, во время поездок по России фотографировал объекты стратегического назначения, собирал сведения о стихийных бедствиях, экологических правонарушениях, невыплате заработной платы, пенсий и пособий в отдельных регионах Российской Федерации и передавал полученные данные советнику посольства Робертсону. Дайте оценку ситуации

6.4. Критерии оценивания

1. Текущая аттестация проводится по результатам работы на практических занятиях.
2. Условием аттестации является присутствие студента на практических занятиях семестра и выполнение заданий.
3. Форму текущей аттестации выбирает преподаватель, ведущий практические занятия.
4. Информация о форме аттестации, о ее процедуре доводится преподавателем до сведения студентов на первом практическом занятии семестра.
5. Формой контроля знаний при проведении промежуточной аттестации является зачет, который проводится в соответствии с графиком учебного процесса.

Более подробно уровни сформированности каждой компетенции по дисциплине и конкретные критерии оценивания приведены в Фонде оценочных средств дисциплины, утвержденном в установленном порядке в дополнение к настоящей рабочей программе.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

7.1. Рекомендуемая литература

7.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.1	Партыка Т. Л., Попов И.И.	Информационная безопасность: учебное пособие (https://znanium.com/catalog/document?id=364624)	Москва : Издательство "ФОРУМ", 2021	ЭБС
Л1.2	Корабельников С. М.	Преступления в сфере информационной безопасности: учебное пособие для вузов (https://urait.ru/bcode/588094)	Москва : Юрайт, 2026	ЭБС

7.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л2.1	Милашевская Е. С.	Уголовная ответственность за преступления в сфере компьютерной информации: монография (https://biblioclub.ru/index.php?page=book&id=142535)	Москва : Лаборатория книги, 2012	ЭБС
Л2.2	Кияев В., Граничин О.	Безопасность информационных систем: курс: учебное пособие (https://biblioclub.ru/index.php?page=book&id=429032)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС

7.2. Перечень ресурсов информационно-телекоммуникационной сети "Интернет"

Э1	Университетская библиотека онлайн [Электронный ресурс] : электронно-библиотечная система (ЭБС) / ООО Директмедиа Паблишинг. URL: http://biblioclub.ru.
Э2	Юрайт [Электронный ресурс] : электронно-библиотечная система (ЭБС) / издательство Юрайт. – URL: https://biblio-online.ru.

7.3 Перечень информационных технологий

7.3.1 Программное обеспечение

Adobe Connect Acrobat

LMS Moodle

Adobe Reader

LibreOffice

7.3.2 Профессиональные базы данных и информационно-справочные системы

1. Научная электронная библиотека eLIBRARY.RU (https://elibrary.ru/defaultx.asp?) eLIBRARY.RU : научная электронная библиотека : сайт. – Москва, 2000 – . – URL: https://elibrary.ru. – Режим доступа: для зарегистрир. пользователей. – Текст : электронный.

2. Справочно-правовая система «КонсультантПлюс» (http://www.consultant.ru/) КонсультантПлюс : справочно- правовая система : база данных / Региональный центр правовой информации Информправо. – Москва, 1992 – . – Режим доступа: из читальных залов библиотеки. – Текст : электронный.

3. Справочно-правовая система «Гарант» (http://www.garant.ru/) ГАРАНТ.РУ : информационно-правовой портал / ООО «НПО ГАРАНТ-СЕРВИС». – Москва, 1990 – . – Режим доступа: из читальных залов библиотеки 1-го корпуса (читальный зал № 3 – ауд. 205, медиацентр – ауд. 206, библиотека юридической литературы – ауд. 215). – Текст : электронный.

8. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Для подготовки и проведения занятий по дисциплине используются следующие объекты и элементы объектов материально-технической базы университета:

- аудитории для проведения лекционных и практических занятий ЧелГУ с имеющимися средствами технического обеспечения занятий;

- учебная библиотека и научный читальный зал ЧелГУ с их средствами и технологиями информационного обеспечения;

Название кабинета Номер аудитории Оборудование

Аудитория для проведения вебинаров ул.Молодогвардейцев, 57а, каб. (110) Персональный компьютер,

Веб-камера,

Колонки

Лингафонный кабинет Ул.Бр.Кашириных, 129, к.428 Специально оборудованный мультимедийный класс

Учебная аудитория для самостоятельной работы Ул.Бр. Кашириных, 129, к.206

Тифлотехническая аудитория ауд. А-28,

ул.Бр.Кашириных, 129

Тифлотехнические средства: брайлевский компьютер с дисплеем и принтером, тифлокомплекс «Читающая машина», телевизионное увеличивающее устройство, тифломагнитолы кассетные (3 шт.) и цифровые диктофоны (6 шт.). Специальное программное обеспечение: программа речевой навигации JAWS, речевые синтезаторы («говорящая мышь»), экранные лупы.

Сурдотехническая аудитория ауд.А-27,

ул. Бр.Кашириных, 129 Радиокласс “Сонет-Р” (на 6 человек), программируемые слуховые аппараты (6 шт.) индивидуального пользования с устройством задания режима работы на компьютере, аудиотехника.

Аудитория адаптивных информационных технологий ауд.А-27,

ул. Бр.Кашириных, 129 Компьютерный класс на 12 мест, интерактивная доска ActiveBoard с системой голосования, акустический усилитель и колонки, мультимедийный проектор, телевизор, видеомагнитофон, устройство видеоконференцсвязи VCONHD3000.

Обучение инвалидов и лиц с ограниченными возможностями здоровья осуществляется с применением следующего специального оборудования:

а) для лиц с нарушением слуха (акустический усилитель и колонки, мультимедийный проектор);

б) для лиц с нарушением зрения (мультимедийный проектор (использование презентаций с укрупненным текстом);

в) для лиц с нарушением опорно-двигательного аппарата (персональные мобильные компьютеры – нетбуки).

В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусмотрено соответствующее количество мест для обучающихся с учетом ограничений их здоровья.

В учебные аудитории обеспечен беспрепятственный доступ для обучающихся инвалидов и обучающихся с ограниченными возможностями здоровья.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Приступая к изучению дисциплины студент должен ясно представлять, что результат обучения зависит не только от работы преподавателей, но и о того, насколько добросовестно он сам подойдет к этому процессу.
Необходимо сразу точно понять критерии оценки всех видов учебной работы, критерии получения экзаменационной оценки.
Формирование умения самостоятельно добывать знания из различных источников, систематизировать полученную информацию, давать оценку конкретной ситуации происходит в течение всего периода обучения через участие

студентов в лекционных и практических занятиях, при выполнении контрольных и курсовых работ. При этом самостоятельная работа студентов играет решающую роль в ходе всего учебного процесса.
Начиная изучать дисциплину необходимо познакомиться с рабочей программой, списком основной и дополнительной литературы, электронных ресурсов. В результате должно сформироваться четкое представление об объеме и характере знаний и компетенций, которыми надо будет овладеть по дисциплине.
Самостоятельная работа обучающегося, включает работу с учебными и учебно-методическими материалами (on-line, off-line), выполнение индивидуальных заданий (off-line), контрольных и курсовых работ (off-line).
При изучении дисциплины следует внимательного познакомиться с вопросами, рекомендуемыми для подготовки к экзамену/зачету. Они ориентируют студента, показывают, что он должен знать по данной дисциплине. Необходимо изучить материал лекций и сопоставить его с трактовками, предлагаемыми в источниках списка рекомендованной (основной и дополнительной) литературы. Следует учитывать тот факт, что время, отводимое на лекционный курс, не позволяет охватить весь учебный курс дисциплины. Поэтому в процессе освоения дисциплины для лучшего усвоения материала необходимо регулярно обращаться к литературным источникам, предлагаемым в библиографическом списке, пользоваться через компьютерную сеть университета и при самостоятельной подготовке в домашних условиях образовательными ресурсами, представленными в разделе 1.5., а также общедоступными Интернет-порталами, содержащими большое количество как научно-популярных, так и специализированных статей, посвященных различным аспектам учебной дисциплины.
При самостоятельном изучении тем следует учитывать следующие советы:
– при первом знакомстве с материалом просмотреть изучаемый текст, представить себе его общее содержание, логику изложения;
– вдумчивое чтение текста надо осуществлять медленно, уясняя прочитанное, выделяя основные идеи. Прочитав материал, попытаться соотнести теорию с примерами из практики;
– при изучении сложного материала необходимо составить тезисы, рабочие записи;
– если в тексте встречаются непонятные термины, необходимо воспользоваться словарем и выяснить значение термина, иначе дальнейшее понимание материала будет осложнено;
– необходимо критически осмысливать прочитанное и изученное, ответить на вопросы, предложенные после каждой темы.
Обучающиеся могут получать консультации преподавателей с использованием средств телекоммуникации:
- очные индивидуальные;
- дистанционные индивидуальные (on-line,off-line);
- дистанционные групповые (on-line,off-line).
Контроль знаний обучающихся осуществляется в форме тестирования. При подготовке к тестированию следует повторить пройденный теоретический материал, выполнить соответствующие задания для самостоятельной работы и тесты для самоконтроля. Контрольные тесты проводятся в определенное время и предусматривают одну попытку.
В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья большое значение имеет индивидуальная работа. Под индивидуальной работой подразумевается две формы взаимодействия с преподавателем: индивидуальная учебная работа (консультации), т.е. дополнительное разъяснение учебного материала и углубленное изучение материала с теми обучающимися, которые в этом заинтересованы. Индивидуальные консультации по предмету является важным фактором, способствующим индивидуализации обучения и установлению контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

10. СПЕЦИАЛЬНЫЕ УСЛОВИЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМИСЯ С ИНВАЛИДНОСТЬЮ И ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Освоение дисциплины инвалидами и лицами с ограниченными возможностями здоровья осуществляется с использованием специальных технических средств и информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося (мобильные специальные технические средства для лиц с нарушениями зрения и с нарушением слуха, ассистивные информационные технологии).
При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации, речевые синтезаторы, экранные лупы).
В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся с инвалидностью и с ограниченными возможностями здоровья. В каждой аудитории, где обучаются инвалиды и лица с ограниченными возможностями здоровья, предусматривается соответствующее количество мест для обучающихся с учетом нарушений их здоровья.
Для освоения дисциплины инвалидам и лицам с ограниченными возможностями здоровья предоставляется доступ к

печатным источникам, имеющимся в научной библиотеке ЧелГУ, с помощью специальных технических средств; доступ с помощью специальных технических и программных средств к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах.

Учебно-методические материалы для обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья предоставляются в формах, адаптированных к ограничениям их здоровья и особенностям восприятия информации.

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий.

При проведении промежуточной аттестации по дисциплине обучающимся с инвалидностью и с ограниченными возможностями здоровья обеспечивается по их заявлению предоставление в доступной форме в зависимости от их индивидуальных особенностей инструкции о порядке проведения промежуточной аттестации, оценочных средств и возможности ответов на задания (письменно на бумаге, набор ответов на компьютере, письменно шрифтом Брайля, с использованием услуг ассистента, устно).

При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья предусматривается использование предоставленных ЧелГУ или собственных технических средств, необходимых им в связи с их индивидуальными особенностями. При необходимости инвалидам и лицам с ограниченными возможностями здоровья предоставляется дополнительное время для подготовки ответа на задания, процедура оценивания результатов обучения по дисциплине может проводиться в несколько этапов.

Рабочая программа дисциплины: Проблемы противодействия информационной преступности
Направление подготовки (специальность): 40.04.01 Юриспруденция

Направленность (профиль): Юрист по уголовным делам

Присваиваемая квалификация (степень): Магистр

Форма обучения: Заочная

Год начала подготовки: 2026

Рабочая программа дисциплины (модуля) одобрена и рекомендована:

Проректор по учебной работе утверждено 27.02.26 А.А. Саламатов

Ученым советом факультета заочного и дистанционного обучения

Протокол заседания № 1 от 12.02.2026

Председатель Ученого совета факультета заочного и дистанционного обучения согласовано Ш.Ш. Ягафаров

Заседанием кафедры современных образовательных технологий

Протокол заседания № 1 от 12.02.2026

И.о. заведующего кафедрой согласовано Н.А. Берг

Автор (составитель) А.В. Штефан

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «13»апреля 2021 г. № 274-1