УТВЕРЖДАЮ
Проректор по учебной работе
/ В.Е. Федоров
«31» 08 2020 г.

Рабочая программа дисциплины (модуля)*

Правовое и криминологическое обеспечение информационной безопасности Российской Федерации

Направление подготовки (специальность)

40.05.01 Правовое обеспечение национальной безопасности

Направленность (профиль)

специализация N 3 "Гражданско-правовая"

Присваиваемая квалификация (степень)

юрист

Форма обучения

заочная

Годы набора 2018, 2019, 2020

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

Челябинск 2020 г.

Рабочая программа дисциплины (модуля) принята:

Ученым советом Институт права

Протокол заседания № 18 «08» 07 2020 г.

Председатель Ученого совета
Института права _____ В.В. Киреев

Секретарь Ученого совета
Института права _____ Л.А. Косенко

Рабочая программа дисциплины (модуля) одобрена и рекомендована кафедрой

Уголовного права и криминологии

Протокол заседания № 17 от «30» 06 2020 г.

И.о. заведующего кафедрой _____ Кадырова Н.Н.

Автор (составитель) _____ к.ю.н., доцент, Никитин Е.В.

Структура рабочей программы соответствует приказу ректора ФГБОУ ВО «ЧелГУ» от «05» декабря 2018 г. № 678-1

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.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Цикл (раздел) ОПОП:	Б1.В.1.04

2.1 Требования к предварительной подготовке обучающегося:

Организационное обеспечение защиты информации

Основы теории национальной безопасности

Криминология

Уголовное право

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

Подготовка к процедуре защиты и процедура защиты выпускной квалификационной работы

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

ОПК-2: способностью реализовывать нормы материального и процессуального права, законодательство Российской Федерации, общепризнанные принципы и нормы международного права в профессиональной деятельности

Знать:

основные информационные ресурсы и технологии, используемые в области защиты государственной тайны и информационной безопасности

Уметь:

применять информационные ресурсы и технологии в процессе получения, поиска, систематизации, обработки и передачи секретной информации

Владеть:

навыками пользования информационными ресурсами и технологиями в процессе получения, поиска, систематизации, обработки и передачи информации

ПК-12: способностью осуществлять профилактику, предупреждение правонарушений, коррупционных проявлений, выявлять и устранять причины и условия, способствующие их совершению

Знать:

методику осуществления профилактики, предупреждения правонарушений и коррупционных проявлений в сфере информационной безопасности

Уметь:

осуществлять профилактику, предупреждение правонарушений в сфере информационной безопасности, выявлять и устранять причины и условия, способствующие их совершению

Владеть:

способностью осуществлять профилактику, предупреждение правонарушений, в сфере информационной безопасности, выявлять и устранять причины и условия, способствующие их совершению

ПК-16: способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

Знать:

требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

Уметь:

соблюдать требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

Владеть:

способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

В результате освоения дисциплины обучающийся должен

3.1	**Знать:**
3.1.1	- основные информационные ресурсы и технологии, используемые в области защиты государственной тайны и информационной безопасности
3.1.2	-методику осуществления профилактики, предупреждения правонарушений и коррупционных проявлений в сфере информационной безопасности
3.1.3	-требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности
3.2	**Уметь:**
3.2.1	- применять информационные ресурсы и технологии в процессе получения, поиска, систематизации, обработки и передачи секретной информации
3.2.2	-соблюдать требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности
3.2.3	-осуществлять профилактику, предупреждение правонарушений в сфере информационной безопасности, выявлять и устранять причины и условия, способствующие их совершению
3.3	**Владеть:**
3.3.1	- навыками пользования информационными ресурсами и технологиями в процессе получения, поиска, систематизации, обработки и передачи информации
3.3.2	- способностью осуществлять профилактику, предупреждение правонарушений, в сфере информационной безопасности, выявлять и устранять причины и условия, способствующие их совершению
3.3.3	-способностью соблюдать в профессиональной деятельности требования нормативных правовых актов в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности

4. ОБЪЕМ ДИСЦИПЛИНЫ (МОДУЛЯ)	
Общая трудоемкость	**5 ЗЕТ**
Часов по учебному плану : 180 в том числе : аудиторные занятия : 18 самостоятельная работа : 149 часов на контроль : 13	Виды контроля на курсах: экзамены 5 зачеты 5

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/	5	2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
1.2	Информационная безопасность в системе обеспечения национальной безопасности /Ср/	5	10	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
1.3	Основные угрозы информационной безопасности /Ср/	5	10	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
1.4	Информация как объект обеспечения безопасности /Ср/	5	10	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
1.5	Зарубежный опыт обеспечения информационной безопасности /Ср/	5	10	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
	Раздел 2. Правовое обеспечение информационной безопасности			
2.1	Правовые средства обеспечения информационной безопасности /Лек/	5	2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2

2.2	Правовые средства обеспечения информационной безопасности /Ср/	5	10	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
2.3	Правовые режимы обеспечения информации ограниченного доступа /Ср/	5	6	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
2.4	Организационно-правовое обеспечение защиты информационных систем /Ср/	5	2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
2.5	Правовые проблемы обеспечения безопасности в сети Интернет /Ср/	5	6	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
2.6	Защита детей от информации, причиняющей вред их здоровью и развитию /Ср/	5	6	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
	Раздел 3. Юридическая ответственность за правонарушения в сфере обеспечения информационной безопасности			
3.1	Дисциплинарная ответственность за информационные правонарушения /Ср/	5	10	Л1.1 Л1.2Л2.2 Л2.3 Э1 Э2
3.2	Гражданско-правовая ответственность за правонарушения в информационной сфере /Ср/	5	10	Л1.1 Л1.2Л2.2 Л2.3 Э1 Э2
3.3	Административные правонарушения в области связи и информации /Пр/	5	4	Л1.1 Л1.2Л2.2 Л2.3 Э1 Э2
3.4	Административные правонарушения в области связи и информации /Ср/	5	10	Л1.1 Л1.2Л2.3 Э1 Э2
3.5	Уголовная ответственность за преступления в сфере информации /Пр/	5	4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
3.6	Уголовная ответственность за преступления в сфере информации /Ср/	5	10	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
	Раздел 4. Криминологическое обеспечение информационной безопасности			
4.1	Понятие, свойства и типология преступности против информационной безопасности /Ср/	5	10	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
4.2	Состояние, структура и динамика преступности против общественной безопасности /Лаб/	5	2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
4.3	Состояние, структура и динамика преступности против общественной безопасности /Ср/	5	2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
4.4	Виктимологические проблемы обеспечения информационной безопасности /Ср/	5	2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
4.5	Личность «информационного» преступника /Пр/	5	2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
4.6	Личность «информационного» преступника /Ср/	5	4	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
4.7	Особенности детерминант преступности против информационной безопасности /Ср/	5	11	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2
4.8	Меры предупреждения и борьбы с преступностью против информационной безопасности /Лаб/	5	2	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2

4.9	Меры предупреждения и борьбы с преступностью против информационной безопасности /Ср/	5	10	Л1.1 Л1.2Л2.1 Л2.2 Л2.3 Э1 Э2

6. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

6.1. Перечень видов оценочных средств

Для текущей аттестации - кейс-задачи, устный опрос, задания для лабораторных работ, 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

Примерные задания для лабораторных работ
1. Начертите схему органов государственной власти, обеспечивающих право доступа к информации.
2. Начертите система органов, обеспечивающих охрану государственной тайны.
3. Как осуществляется взаимодействие органов местного самоуправления и органов государственной власти в условиях информационного общества.
4. Рассчитайте количественные показатели преступности в информационной сфере в Челябинской области и России.
5. В инфографике покажите качественные показатели преступности в информационной сфере в Челябинской области и России

6.3. Типовые контрольные вопросы и задания для промежуточной аттестации

Примерные вопросы для собеседования (зачет)
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

Примерные вопросы для собеседования (экзамен)
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 и экзамен, проводятся 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

	Авторы, составители	Заглавие	Издательство, год	Ресурс
Л1.1	Баранова Е.К., Бабаш А.В.	Актуальные вопросы защиты информации: монография (http://znanium.com/catalog/document?id=348464)	Москва : Издательский Центр РИОР, 2020	ЭБС
Л1.2	Овчинский В.С.	Криминология цифрового мира: учебник (http://znanium.com/catalog/document?id=347769)	Москва : ООО "Юридическое издательство Норма", 2020	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 (http://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 (http://biblioclub.ru/index.php?page=book&id=429032)	Москва : Национальный Открытый Университет «ИНТУИТ», 2016	ЭБС
Л2.3	Баранова Е.К., Бабаш А.В.	Информационная безопасность и защита информации: учебное пособие (http://znanium.com/catalog/document?id=359537)	Москва : Издательский Центр РИОР, 2020	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

MS Office365

Adobe Connect Acrobat

LMS Moodle

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 реализации дисциплины используются учебные аудитории для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также помещения для самостоятельной работы. Специальные помещения укомплектованы специализированной мебелью и техническими средствами обучения, служащими для представления учебной информации большой аудитории. Учебные аудитории для реализации программы предусмотрены учебным планом по направлению подготовки (специальности) и соответствуют действующим санитарным и противопожарным нормам и правилам.

Учебные аудитории укомплектованы специальной мебелью и техническими средствами обучения (демонстрационным оборудованием) для занятий различного типа и (или) применения дистанционных образовательных технологий.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду университета.

Реализация образовательной программы обеспечена необходимым комплектом лицензионного программного обеспечения: СПС Консультант плюс и СПС Гарант – открыт постоянный доступ для обучающихся в компьютерном классе.

В университете имеется библиотека юридической литературы, электронная библиотека и банк данных учебно- методической литературы (первоисточников, монографической и комментирующей литературы, статей, нормативных актов и справочных материалов), читальный зал юридической литературы.

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

Основными формами обучения по дисциплине являются лекции и практические занятия; немаловажное значение имеет и самостоятельная работа студентов.

Лекции составляют основу теоретической подготовки обучающихся, в ходе лекции излагаются систематизированные научные знания по дисциплине, обращается внимание на наиболее сложные и проблемные вопросы. Лекция стимулирует активную познавательную деятельность обучающихся, помогает сформировать творческое мышление при изучении дисциплины.

Практические занятия способствуют углублению и закреплению знаний, полученных на лекциях и в процессе самостоятельной работы. В ходе занятий обучаемые учатся творчески мыслить, грамотно, логично и аргументированно излагать свои взгляды по спорным вопросам темы, рассматривать доводы других участников дискуссии.

Данный вид занятий помогает привить навыки самостоятельной работы, овладеть культурой речи и ораторским искусством и позволяет преподавателю, ведущему занятия, контролировать ход изучения дисциплины.

При подготовке к практическому занятию следует чаще обращаться к справочной литературе, иногда к литературе по смежным наукам (в нашем случае, к уголовному праву, криминологии и др.), полнее использовать консультации преподавателя. В ходе практического занятия в первую очередь студенты обсуждают теоретические вопросы. Затем учащиеся сообщают варианты выполненных заданий самостоятельной работы с соответствующей аргументацией и обоснованием ссылками на законодательство, которые коллективно обсуждаются в порядке свободной дискуссии.

Важно, чтобы каждый студент стремился к активному участию в обсуждении проблем и решении задач, чтобы в ходе практического занятия не осталось непонятных вопросов. На практическом занятии преподаватель может дать новые дополнительные задачи, которые необходимо решить здесь же, и тем самым проверить, насколько глубоко освоены теоретические вопросы по теме и нормативный материал.

Следует внимательно слушать вступительное и заключительное слово руководителя практического занятия, все его замечания. Наиболее важные из них полезно записать. Четкое следование данным рекомендациям позволит студенту успешно освоить материал курса.

Самостоятельная работа обучаемых заключается в повторении материала, изученного на лекционных, семинарских и практических занятиях, выполнении заданий, полученных в ходе лекции и при подготовке к семинарским и практическим занятиям.

В освоении дисциплины 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, и индивидуальная воспитательная работа. Индивидуальные консультации по предмету является важным фактором, способствующим индивидуализации обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с ограниченными возможностями здоровья.

В случае применения при обучении дисциплины электронного обучения, дистанционных образовательных технологий общение обучающихся и преподавателя осуществляется в режиме реального времени (форумы, электронная почта, сотовая связь) и отложенного времени (системы дистанционного обучения Moodle, электронная почта, форумы. Большую часть времени обучающиеся самостоятельно работают с учебно-методическими материалами. Студенты имеют возможность консультироваться с преподавателем по всем вопросам, возникающим в ходе самостоятельной работы посредством системы дистанционного обучения Moodle, электронной почты, сотовой связи, форумов. Доступ обучающегося к учебным ресурсам в режиме отложенного времени, самостоятельной работы осуществляется через сеть Интернет в удобном для него месте, времени и темпе).

При обучении лиц с ограниченными возможностями здоровья электронное обучение, дистанционные образовательные технологии предусматривают возможность приема-передачи информации в доступных для них формах.

Реализация дисциплины с применением электронного обучения, дистанционных образовательных технологий (далее – ЭО, ДОТ) осуществляется на основании «Положения о реализации основных и дополнительных образовательных программ с применением электронного обучения и дистанционных образовательных технологий в федеральном государственном бюджетном образовательном учреждении высшего образования «Челябинский государственный университет», «Положения о порядке зачета обучающимися по основным профессиональным образовательным программам высшего образования в ФГБОУ ВО «ЧелГУ» результатов освоения в организациях, осуществляющих

образовательную деятельность, учебных предметов, курсов, дисциплин (модулей), практик, дополнительных образовательных программ» посредством электронной информационно-образовательной среды ФГБОУ ВО «ЧелГУ». В исключительных случаях (форс-мажор и т.п.) при реализации образовательной деятельности с применением ЭО, ДОТ могут применять компоненты, не входящие в перечень электронной информационно- образовательной среды.

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 голо информационных технологий, предоставляемых Ресурсным учебно-методическим центром по обучению инвалидов и лиц с ограниченными возможностями здоровья ЧелГУ по запросу обучающегося.

1. Мобильные специальные технические средства для лиц с нарушениями зрения: портативный компьютер с вводом/выводом шрифтом Брайля с синтезатором речи «ElBraile-W14J G2»; ноутбуки с программной экранного доступа NVDA; электронные увеличители для удаленного просмотра; видеоувеличители портативные; тифлоплеер; цифровые диктофоны.
2. Мобильные специальные технические средства для лиц с нарушениями слуха: система свободного звукового поля со встроенной совместимостью с FM-устройствами; радиоклассы «Сонет-РСМ» с передатчиком, заушным индуктором и индукционной петлей; система информационная для слабослышащих переносная «Исток» А2 со встроенным плеером – звуковым информатором; документ-камера; программируемые слуховые аппараты индивидуального пользования.
3. Ассистивные информационные технологии: программное обеспечение экранного доступа с синтезом речи NVDA; программы экранного увеличения; программы речевого синтеза для компьютеров и ноутбуков; программы речевого синтеза для мобильных устройств; экранная клавиатура; экранная лупа.

При необходимости для обучающихся с нарушениями зрения на рабочих местах для проведения практических или лабораторных занятий устанавливается специальное программное обеспечение (программа речевой навигации NVDA, речевые синтезаторы, экранные лупы).

В учебные аудитории обеспечивается беспрепятственный доступ для обучающихся инвалидов и обучающихся 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 к электронным источникам, представленным в форме электронного документа в фонде научной библиотеки ЧелГУ или электронно-библиотечных системах, с помощью специальных технических и программных средств (рабочее место для незрячего пользователя с программным обеспечением экранного доступа с синтезом речи NVDA, рабочее место с компьютерным роллером и клавиатурой Clevy с большими кнопками и с разделяющей клавиши накладкой).

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

Для лиц с нарушениями зрения:
- в печатной форме увеличенным шрифтом,
- в форме электронного документа,
- в форме аудиофайла,
- в печатной форме шрифтом Брайля.

Для лиц с нарушениями слуха:
- в печатной форме,
- в форме электронного документа.

Для лиц с нарушениями опорно-двигательного аппарата:
- в печатной форме,
- в форме электронного документа,
- в форме аудиофайла.

Данный перечень может быть конкретизирован в зависимости от контингента обучающихся.

Для инвалидов и лиц с ограниченными возможностями здоровья освоение дисциплины может быть частично или полностью осуществлено с использованием дистанционных образовательных технологий (Moodle, Adobe Connect Pro и пр.).

В освоении дисциплины инвалидами и лицами с ограниченными возможностями здоровья используется 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, и индивидуальная воспитательная работа. Индивидуальные консультации направлены на индивидуализацию обучения и установлению воспитательного контакта между преподавателем и обучающимся инвалидом или обучающимся с

ограниченными возможностями здоровья.
При проведении процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья по дисциплине обеспечивается выполнение следующих дополнительных требований в зависимости от индивидуальных особенностей, обучающихся:
а) инструкция по порядку проведения процедуры оценивания предоставляется в доступной форме (устно, в письменной форме, в письменной форме шрифтом Брайля, устно с использованием услуг сурдопереводчика);
б) доступная форма предоставления заданий оценочных средств (в печатной форме, в печатной форме увеличенным шрифтом, в печатной форме шрифтом Брайля, в форме электронного документа, задания зачитываются ассистентом, задания предоставляются с использованием сурдоперевода);
в) доступная форма предоставления 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 технических средств, необходимых им в связи с их индивидуальными особенностями. Эти средства могут быть предоставлены ЧелГУ или могут использоваться собственные технические средства. 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.
Проведение процедуры оценивания результатов обучения инвалидов и лиц с ограниченными возможностями здоровья допускается с использованием дистанционных образовательных технологий.