

Программу составил(и):

к.ю.н., доцент, Субачев Сергей Юрьевич

Рецензент(ы):

кэн, доцент заместитель начальника отдела по финансовому и фондовому рынку и жилищным программам управления экономики администрации и муниципального образования город Краснодар, Макаренко Ю. Г.; первый заместитель начальника управления инвестиций и развития малого и среднего предпринимательства администрации муниципального образования город Краснодар, начальник отдела муниципально-частного партнерства, Алешин А.С.

Рабочая программа дисциплины

Информационное общество и обеспечение информационной безопасности

разработана в соответствии с ФГОС ВО:

Федеральный государственный образовательный стандарт высшего образования - бакалавриат по направлению подготовки 40.03.01 Юриспруденция (приказ Минобрнауки России от 13.08.2020 г. № 1011)

составлена на основании учебного плана:

40.03.01 Юриспруденция

утвержденного учёным советом вуза от 20.11.2023 протокол № 3.

Рабочая программа одобрена на заседании кафедры

Кафедра математики и вычислительной техники

Протокол от 11.11.2023 г. № 4

Зав. кафедрой Исикова Наталья Павловна

Согласовано с представителями работодателей на заседании НМС, протокол № 3 от 20.11.2023.

Председатель НМС проф. Павелко Н.Н.

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)	
1.1	Целью учебной дисциплины «Информационное общество и обеспечение
1.2	информационной безопасности» является приобретение студентами знаний, навыков и умений,
1.3	связанных с правовыми и программно-техническими проблемами защиты информации
1.4	государственных и негосударственных организаций и учреждений.
Задачи: Задачи дисциплины:	
- определение понятийного аппарата, используемого в области обеспечения безопасности информации в компьютерных системах;	
- систематизация теоретических знаний по обеспечению безопасности информации в системах управления, использующих современные информационные технологии;	
- выявление сущности, целей, задач и места методов и средств защиты информационных процессов в компьютерных системах в общей системе обеспечения безопасности информации на объектах информатизации;	
- изучение основных принципов применения методов и средств защиты информации при организации защиты информационных процессов в компьютерных системах;	
- изучение нормативно-руководящих документов, регламентирующих вопросы обеспечения безопасности информации в автоматизированных системах;	
- развитие у обучаемых управленческих и инженерных навыков обоснованного принятия решений по организации комплексной защиты информации, оценке защищенности и управления процессами защиты в автоматизированных системах.	

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ	
Цикл (раздел) ОП:	Б1.О.10
2.1	Требования к предварительной подготовке обучающегося:
2.1.1	Уголовное право
2.1.2	Информационное общество и обеспечение информационной безопасности
2.1.3	Математика
2.1.4	Информатика и методы математического анализа
2.2	Дисциплины (модули) и практики, для которых освоение данной дисциплины (модуля) необходимо как предшествующее:
2.2.1	Противодействие коррупции
2.2.2	Выполнение, подготовка к процедуре защиты и защита выпускной квалификационной работы
2.2.3	Производственная практика: преддипломная практика
2.2.4	Уголовный процесс
2.2.5	Криминалистика
2.2.6	Налоговые расследования
2.2.7	Противодействие коррупции
2.2.8	Производственная практика: правоприменительная практика
2.2.9	Информационное обеспечение правовых систем

3. ФОРМИРУЕМЫЕ КОМПЕТЕНЦИИ, ИНДИКАТОРЫ ИХ ДОСТИЖЕНИЯ и планируемые результаты обучения	
ОПК-8: Способен целенаправленно и эффективно получать юридически значимую информацию из различных источников, включая правовые базы данных, решать задачи профессиональной деятельности с применением информационных технологий и с учетом требований информационной безопасности	
ОПК-8.1: Способен получать юридически значимую информацию из различных источников с применением информационных технологий, включая правовые базы данных, обрабатывать и систематизировать ее в соответствии с поставленной целью	
Знать	
Уровень 1	юридически значимую информацию из различных источников с применением информационных технологий, включая правовые базы данных, обрабатывать и систематизировать ее на достаточном уровне
Уровень 2	юридически значимую информацию из различных источников с применением информационных технологий, включая правовые базы данных, обрабатывать и систематизировать ее на среднем уровне
Уровень 3	юридически значимую информацию из различных источников с применением информационных технологий, включая правовые базы данных, обрабатывать и систематизировать ее на высоком уровне
Уметь	
Уровень 1	получать и анализировать юридически значимую информацию из различных источников с применением информационных технологий, включая правовые базы данных, обрабатывать и систематизировать ее на достаточном уровне

Уровень 2	получать и анализировать юридически значимую информацию из различных источников с применением информационных технологий, включая правовые базы данных, обрабатывать и систематизировать ее на среднем уровне
Уровень 3	получать и анализировать юридически значимую информацию из различных источников с применением информационных технологий, включая правовые базы данных, обрабатывать и систематизировать ее на высоком уровне
Владеть	
Уровень 1	навыками по получению и анализе юридически значимую информацию из различных источников с применением информационных технологий, включая правовые базы данных, обрабатывать и систематизировать ее на достаточном уровне
Уровень 2	навыками по получению и анализе юридически значимую информацию из различных источников с применением информационных технологий, включая правовые базы данных, обрабатывать и систематизировать ее на среднем уровне
Уровень 3	навыками по получению и анализе юридически значимую информацию из различных источников с применением информационных технологий, включая правовые базы данных, обрабатывать и систематизировать ее на высоком уровне
ОПК-8.2: Способен решать задачи профессиональной деятельности с учетом требований информационной безопасности	
Знать	
Уровень 1	способы решения задач профессиональной деятельности с учетом требований информационной безопасности на достаточном уровне
Уровень 2	способы решения задач профессиональной деятельности с учетом требований информационной безопасности на среднем уровне
Уровень 3	способы решения задач профессиональной деятельности с учетом требований информационной безопасности на высоком уровне
Уметь	
Уровень 1	решать задачи профессиональной деятельности с учетом требований информационной безопасности на достаточном уровне
Уровень 2	решать задачи профессиональной деятельности с учетом требований информационной безопасности на среднем уровне
Уровень 3	решать задачи профессиональной деятельности с учетом требований информационной безопасности на высоком уровне
Владеть	
Уровень 1	навыками по решению задач профессиональной деятельности с учетом требований информационной безопасности на достаточном уровне
Уровень 2	навыками по решению задач профессиональной деятельности с учетом требований информационной безопасности на среднем уровне
Уровень 3	навыками по решению задач профессиональной деятельности с учетом требований информационной безопасности на высоком уровне

ПК-4: Способен выполнять должностные обязанности по обеспечению законности, правопорядка, безопасности личности, общества и государства

ПК-4.1: Способен соблюдать требования законодательства по обеспечению законности и правопорядка, безопасности личности, общества, государства

Знать	
Уровень 1	требования законодательства по обеспечению законности личности, общества, государства
Уровень 2	требования законодательства по обеспечению законности и правопорядка личности, общества, государства
Уровень 3	требования законодательства по обеспечению законности и правопорядка, безопасности личности, общества, государства
Уметь	
Уровень 1	соблюдать требования законодательства по обеспечению законности и правопорядка, безопасности личности, общества, государства допуская минимальные ошибки
Уровень 2	соблюдать требования законодательства по обеспечению законности и правопорядка, безопасности личности, общества, государства допуская недочеты
Уровень 3	соблюдать требования законодательства по обеспечению законности и правопорядка, безопасности личности, общества, государства не допуская ошибки
Владеть	
Уровень 1	навыками применять законодательств в обеспечению законности личности, общества, государства
Уровень 2	навыками применять законодательств в обеспечению законности и правопорядка личности, общества, государства
Уровень 3	навыками применять законодательств в обеспечению законности и правопорядка, безопасности личности,

	общества, государства
ПК-4.2: Способен выявлять, пресекать, раскрывать и расследовать преступления и иные правонарушения	
Знать	
Уровень 1	принципы, способы и методы выявления, пресечения, раскрытия и расследования преступлений и иных правонарушений на минимально допустимом уровне
Уровень 2	принципы, способы и методы выявления, пресечения, раскрытия и расследования преступлений и иных правонарушений на среднем уровне
Уровень 3	принципы, способы и методы выявления, пресечения, раскрытия и расследования преступлений и иных правонарушений на высоком уровне
Уметь	
Уровень 1	Способен выявлять преступления и иные правонарушения
Уровень 2	Способен выявлять, пресекать, раскрывать преступления и иные правонарушения
Уровень 3	Способен выявлять, пресекать, раскрывать и расследовать преступления и иные правонарушения
Владеть	
Уровень 1	навыками выявлять, пресекать, раскрывать и расследовать преступления и иные правонарушения на допустимом уровне
Уровень 2	навыками выявлять, пресекать, раскрывать и расследовать преступления и иные правонарушения на среднем уровне
Уровень 3	навыками выявлять, пресекать, раскрывать и расследовать преступления и иные правонарушения на высоком уровне

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

Код занятия	Наименование разделов и тем /вид занятия/	Семестр / Курс	Часов	Компетенции	Литература и эл. ресурсы	Практ . подг.
	Раздел 1. Содержание					
1.1	1. Основные определения и критерии классификации угроз и атак /Лек/	5	8	ОПК-8.1 ОПК-8.2 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2	
1.2	1. Основные определения и критерии классификации угроз и атак /Пр/	5	4	ОПК-8.1 ОПК-8.2 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2	
1.3	1. Основные определения и критерии классификации угроз и атак /Лаб/	5	4	ОПК-8.1 ОПК-8.2 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.5Л2.1 Л2.2 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2	
1.4	2. Безопасность в Глобальной сети Internet /Лек/	5	8	ОПК-8.1 ОПК-8.2 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2	
1.5	2. Безопасность в Глобальной сети Internet /Пр/	5	4	ОПК-8.1 ОПК-8.2 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.5Л2.1 Л2.2 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2	
1.6	2. Безопасность в Глобальной сети Internet /Лаб/	5	4	ОПК-8.1 ОПК-8.2 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.5Л2.1 Л2.2 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2	
1.7	3. Противодействие несанкционированному доступу к источникам информации /Лек/	5	8	ОПК-8.1 ОПК-8.2 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2	
1.8	3. Противодействие несанкционированному доступу к источникам информации /Пр/	5	4	ОПК-8.1 ОПК-8.2 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2	

1.9	3. Противодействие несанкционированному доступу к источникам информации /Лаб/	5	4	ОПК-8.1 ОПК-8.2 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.5Л2.1 Л2.2 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2
1.10	4. Методы криптографической защиты информации /Лек/	5	8	ОПК-8.1 ОПК-8.2 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2
1.11	4. Методы криптографической защиты информации /Пр/	5	4	ОПК-8.1 ОПК-8.2 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.5Л2.1 Л2.2 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2
1.12	4. Методы криптографической защиты информации /Лаб/	5	4	ОПК-8.1 ОПК-8.2 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.5Л2.1 Л2.2 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2
Раздел 2. Контактная работа на аттестации (в период экз. сессий)					
2.1	/КАЭ/	5	0,3	ОПК-8.1 ОПК-8.2 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2
2.2	/Консл/	5	1	ОПК-8.1 ОПК-8.2 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2
2.3	/Ср/	5	8	ОПК-8.1 ОПК-8.2 ПК-4.1 ПК-4.2	Л1.1 Л1.2 Л1.3 Л1.4 Л1.5Л2.1 Л2.2 Л2.3 Л2.4 Л2.5Л3.1 Л3.2 Э1 Э2

5. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

5.1. Контрольные вопросы и задания

1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
4. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
5. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
6. Понятие политики безопасности информационных систем. Назначение политики безопасности.
7. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
8. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
9. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
10. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
11. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
12. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
13. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
14. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
15. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
16. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
17. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
18. Биометрические средства идентификации и аутентификации пользователей.
19. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
20. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.
21. Понятие электронной цифровой подписи. Процедуры формирования цифровой подписи.
22. Законодательный уровень применения цифровой подписи.

23. Методы несимметричного шифрования. Использование несимметричного шифрования для обеспечения целостности данных.
24. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы.
25. Место информационной безопасности экономических систем в национальной безопасности страны. Концепция информационной безопасности.
26. Причины нарушения безопасности информации при ее обработке криптографическими средствами.
27. Понятие атаки на систему информационной безопасности. Особенности локальных атак.
28. Распределенные информационные системы. Удаленные атаки на информационную систему.
29. Каналы передачи данных. Утечка информации. Атаки на каналы передачи данных.
30. Физические средства обеспечения информационной безопасности.
31. Электронная почта. Проблемы обеспечения безопасности почтовых сервисов и их решения.
32. Вирусы и методы борьбы с ними. Антивирусные программы и пакеты.
33. Программно-аппаратные защиты информационных ресурсов в Интернет. Межсетевые экраны, их функции и назначения.
34. Виртуальные частные сети, их функции и назначение.

5.2. Темы письменных работ

1. Классификация угроз информационной безопасности автоматизированных систем по базовым признакам.
2. Угроза нарушения конфиденциальности. Особенности и примеры реализации угрозы.
3. Угроза нарушения целостности данных. Особенности и примеры реализации угрозы.
4. Угроза отказа служб (угроза отказа в доступе). Особенности и примеры реализации угрозы.
5. Угроза раскрытия параметров системы. Особенности и примеры реализации угрозы.
6. Понятие политики безопасности информационных систем. Назначение политики безопасности.
7. Основные типы политики безопасности доступа к данным. Дискреционные и мандатные политики.
8. Требования к системам криптографической защиты: криптографические требования, требования надежности, требования по защите от НСД, требования к средствам разработки.
9. Законодательный уровень обеспечения информационной безопасности. Основные законодательные акты РФ в области защиты информации.
10. Функции и назначение стандартов информационной безопасности. Примеры стандартов, их роль при проектировании и разработке информационных систем.
11. Критерии оценки безопасности компьютерных систем («Оранжевая книга»). Структура требований безопасности. Классы защищенности.
12. Единые критерии безопасности информационных технологий. Понятие профиля защиты. Структура профиля защиты.
13. Единые критерии безопасности информационных технологий. Проект защиты. Требования безопасности (функциональные требования и требования адекватности).
14. Административный уровень защиты информации. Задачи различных уровней управления в решении задачи обеспечения информационной безопасности.
15. Процедурный уровень обеспечения безопасности. Авторизация пользователей в информационной системе.
16. Идентификация и аутентификация при входе в информационную систему. Использование парольных схем. Недостатки парольных схем.
17. Идентификация и аутентификация пользователей. Применение программно-аппаратных средств аутентификации (смарт-карты, токены).
18. Биометрические средства идентификации и аутентификации пользователей.
19. Аутентификация субъектов в распределенных системах, проблемы и решения. Схема Kerberos.
20. Аудит в информационных системах. Функции и назначение аудита, его роль в обеспечении информационной безопасности.

5.3. Фонд оценочных средств

1. Информационное общество - это:
 - а) общество, в котором большая часть населения имеет дома персональный компьютер и умеет работать на нем;
 - б) общество, в котором большая часть населения занята получением, переработкой, передачей и хранением информации;
 - в) общество, в котором большая часть населения умеет получать информацию из любых информационных источников.
2. С чем связана первая информационная революция?
 - а) с изобретением колеса; б) с развитием торговли; в) с изобретением письменности.
3. Какая информационная революция позволила оперативно передавать и накапливать информацию?
 - а) первая; б) четвертая; в) третья.

12. Укажите особо опасные виды компьютерных вирусов:

а) Черви; б) Троянцы.

Тест по теме "Информационное общество и информационная безопасность"

Вариант 2

1. Сколько всего в истории человечества случилось информационных революций?

а) 4; б) 3; в) 5.

2. С чем связана вторая информационная революция?

а) с изобретением микропроцессоров; б) с изобретением книгопечатания; в) с изобретением электричества.

3. Умение целенаправленно работать с информацией – это...

а) информационная культура; б) информационные ресурсы; в) информационная грамотность.

4. Какая программа позволяет работать с мультимедийными объектами?

а) Microsoft Excel; б) Microsoft PowerPoint; в) Microsoft Access.

5. На что распространяется охрана интеллектуальных и авторских прав в сфере информатики?

а) на идеи и принципы, лежащие в основе компьютерной программы;

б) на идеи и принципы алгоритма и организации интерфейса;

в) на все виды программ для компьютера.

6. Чего может добиться автор компьютерной программы в отношении организаций или пользователей, нарушивших авторские права?

а) Возмещения причиненных убытков и выплаты компенсации;

б) Привлечения нарушителей к уголовной ответственности;

в) Конфискации имущества.

7. На какие группы делятся программы по их правовому статусу?

а) Бесплатные, условно бесплатные и лицензионные;

б) Лицензионные, условно бесплатные и свободно распространяемые программы;

в) Платные, лицензионные и бесплатные.

8. С какой целью предлагают разработчики условно бесплатные программы?

- а)С целью доработки этих программ;
 б)С целью предложения принципиально новых технологий;
 в)С целью рекламы и продвижения программ на рынок.

9.Что обычно используется для защиты от несанкционированного доступа к данным на компьютере?

- а)Логин и пароль; б)Шифровой код; в)Только пароль.

10.Что такое инсталляция программы?

- а)Удаление программы с компьютера;
 б)Установка программы на компьютер;
 в)Копирование программы

11.Для предотвращения нелегального копирования программ используется:

- а)Программный ключ; б)Дистрибутив; в)Пароль.

12.Что предохраняет компьютер, подключенный к Интернету, от сетевых вирусов и хакерских атак?

- а)Межсетевой экран; б)Сервер; в)Антивирусная защита.

5.4. Перечень видов оценочных средств

Опрос;
 Реферат;
 Тестирование.

Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа на теоретический вопрос. Задание с выбором одного варианта ответа (ОВ, в задании данного типа предлагается несколько вариантов ответа, среди которых один верный. Задания со свободно конструируемым ответом (СКО) предполагает составление развернутого ответа, включающего полное решение задачи с пояснениями.

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

6.1. Рекомендуемая литература

6.1.1. Основная литература

	Авторы, составители	Заглавие	Издательство, год
Л1.1	Дроздов В. Ю., Хлыстова Н. Б.	Криминология и предупреждение правонарушений: Учебник	Москва: КноРус, 2020, URL: https://book.ru/book/935895
Л1.2	Гишинский Я. И., под ред., Орлов В. Н., под ред., Артеменко Н. В., Гуринская А. Л., Дикаева М. С., Закаляпина Л. А., Морозова И. В., Петровский А. В., Скиба А. П., Татьяна В. П., Цэнгэл С. Д., Щербакова Л. М.	Криминология: Учебник	Москва: Юстиция, 2019, URL: https://book.ru/book/930550
Л1.3	Дроздов В. Ю., Хлыстова Н. Б.	Криминология: Учебник	Москва: КноРус, 2019, URL: https://book.ru/book/932555

	Авторы, составители	Заглавие	Издательство, год
Л1.4	Дроздов В. Ю., Хлыстова Н. Б.	Криминология: Учебник	Москва: КноРус, 2021, URL: https://book.ru/book/936308
Л1.5	Гладких В. И., под ред., Абызов Р. М., Алиев В. М., Аминов Д. И., Гончарова М. В., Бакрадзе А. А., Жигарев Е. С., Иванцов С. В., Ларичев В. Д., Молчанова Т. В., Моргуленко Е. А., Резчиков В. Л., Сбирунов П. Н., Уткин В. А., Уткина Е. В., Ходусов А. А., Шумов Р. Н.	Криминология: Учебник	Москва: Юстиция, 2022, URL: https://book.ru/book/945119

6.1.2. Дополнительная литература

	Авторы, составители	Заглавие	Издательство, год
Л2.1	Попова Е.З.	Криминология: Учебное пособие	Москва: Российский государственный университет правосудия, 2017, URL: http://znanium.com/catalog/document?id=335532
Л2.2	Серегина Е.В., Москалева Е.Н.	Криминология: Учебное пособие	Москва: Российский государственный университет правосудия, 2018, URL: http://znanium.com/catalog/document?id=335590
Л2.3	Овчинский В.С.	Криминология цифрового мира: Учебник	Москва: ООО "Юридическое издательство Норма", 2020, URL: http://znanium.com/catalog/document?id=347769
Л2.4	Долгова А.И.	Криминология: Учебник	Москва: ООО "Юридическое издательство Норма", 2019, URL: http://znanium.com/catalog/document?id=353572
Л2.5	Долгова А.И.	Криминология: Учебник	Москва: ООО "Юридическое издательство Норма", 2020, URL: http://znanium.com/catalog/document?id=365147

6.1.3. Методические разработки

	Авторы, составители	Заглавие	Издательство, год
Л3.1	Долгова А.И.	Криминология: Учебное пособие	Москва: ООО "Юридическое издательство Норма", 2023, URL: https://znanium.com/catalog/document?id=427288
Л3.2	Николаева Ю. В., под ред., Батюкова В. Е., Гримальская С. А., Красненкова Е. В., Малахова В. Ю.	Криминология. Общая часть: Учебное пособие	Москва: КноРус, 2022, URL: https://book.ru/book/943794

6.2. Электронные учебные издания и электронные образовательные ресурсы

Э1	МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РОССИЙСКОЙ ФЕДЕРАЦИИ. - Режим доступа: https://мвд.рф/		
Э2	ГЕНЕРАЛЬНАЯ ПРОКУРАТУРА РОССИЙСКОЙ ФЕДЕРАЦИИ ПОРТАЛ ПРАВОВОЙ СТАТИСТИКИ. - Режим доступа: http://crimestat.ru/		

6.3.1. Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства

6.3.1.1	Windows 10 Pro RUS Операционная система – Windows 10 Pro RUS Подписка Microsoft Imagine Premium – Order №143659 от 12.07.2021		
6.3.1.2	7-Zip Архиватор 7-Zip Программное обеспечение по лицензии GNU GPL		

6.3.1.3	Яндекс Браузер Браузер Яндекс Браузер Лицензионное соглашение на использование программ Яндекс Браузер https://yandex.ru/legal/browser_agreement/
6.3.1.4	Mozilla Firefox Браузер Mozilla Firefox Программное обеспечение по лицензии GNU GPL
6.3.1.5	LibreOffice Офисный пакет LibreOffice Программное обеспечение по лицензии GNU GPL
6.3.1.6	LibreCAD САПР для 2-мерного черчения и проектирования LibreCAD Программное обеспечение по лицензии GNU GPL
6.3.1.7	Inkscape Графический редактор Inkscape Программное обеспечение по лицензии GNU GPL
6.3.1.8	Notepad++. Текстовый редактор Notepad++. Программное обеспечение по лицензии GNU GPL
6.3.1.9	1С:Предприятие 8. Комплект 1С:Предприятие 8. Комплект для обучения в высших и средних учебных заведениях. Сублицензионный договор № 32/180913/005 от 18.09.2013. (Первый БИТ)
6.3.1.1 0	Kaspersky Endpoint Security Антивирусное ПО Kaspersky Endpoint Security для бизнеса Стандартный (350шт). Договор № ПР-00037842 от 4 декабря 2023 г. (ООО Прима АйТи)
6.3.1.1 1	Visual Studio Code Редактор исходного кода, разработанный Microsoft для Windows, Linux и macOS Программное обеспечение по лицензии GNU GPL
6.3.1.1	Blender ПО для создания трёхмерной компьютерной графики Программное обеспечение по лицензии GNU GPL
6.3.1.1	Gimp Графический редактор Gimp Программное обеспечение по лицензии GNU GPL
6.3.1.1	Maxima Математический пакет Maxima Программное обеспечение по лицензии GNU GPL
6.3.1.1 5	Oracle VM VirtualBox VM VirtualBox — программный продукт виртуализации для операционных систем Программное обеспечение по лицензии GNU GPL
6.3.1.1	StarUML VI Case средство UML Программное обеспечение по лицензии GNU GPL
6.3.1.1	PostgreSQL Система управления базами данных Программное обеспечение по лицензии GNU GPL
6.3.1.1 8	Diptrace Программное обеспечение EDA/CAD для создания принципиальных схем и печатных плат Лицензия для образовательной организации. Лицензионное соглашение с окончательным пользователем ООО «Новарм»
6.3.1.1	MecSoft FreeMILL for VisualCAM Программное обеспечение для программирования станков с ЧПУ Freeware
6.3.1.2 0	Arduino Software (IDE) Интегрированная среда разработки, предназначенная для создания и загрузки программ на Arduino-совместимые платы, а также на платы других производителей Программное обеспечение по лицензии GNU GPL
6.3.1.2 1	NetBeans IDE Интегрированная среда разработки приложений на языках программирования Java, Python, PHP, JavaScript, C, C++, Ада и ряда других Программное обеспечение по лицензии GNU GPL
6.3.1.2	ZEAL Оффлайн-браузер для просмотра документации Программное обеспечение по лицензии GNU GPL
6.3.1.2 3	ARIS Express Инструмент моделирования для анализа и управления бизнес-процессами Программное обеспечение по лицензии GNU GPL
6.3.1.2 4	AnyLogic Программное обеспечение для имитационного моделирования Программное обеспечение по лицензии GNU GPL
6.3.1.2 5	Archimate Инструментарий моделирования для создания моделей и эскизов ArchiMate. ArchiMate Non-Commercial License
6.3.1.2 6	SMath Studio Программа для вычисления математических выражений и построения графиков функций Программное обеспечение по лицензии GNU GPL
6.3.1.2 7	Комплекс КРЕДО - Землеустройство и кадастры Комплекс для ВУЗов-Землеустройство и кадастры: Кредо топограф, кредо трансформ, кредо транскор, кредо кадастр, кредо конвертер Акт № 123 от 01.11.2018. Сертификат от 24.08.2018
6.3.1.2 8	Klite Mega Codec Pack Универсальный набор кодеков и утилит для просмотра и обработки аудио- и видеофайлов Freeware
6.3.1.2	CDBurnerXP ПО для записи CD, DVD, HD DVD и Blu-ray Freeware
6.3.1.3	Java 8 Программная платформа Java Программное обеспечение по лицензии GNU GPL
6.3.1.3	PDF24 Creator Приложение для создания и редактирования документов в формате PDF Freeware
6.3.1.3	CCleaner Утилита для очистки ПК Freeware
6.3.1.3 3	Консоль Kaspersky Security Center Консоль администрирования Kaspersky Security Center Договор № ПР-00035750 от 13 декабря 2022г. (ООО Прима АйТи)
6.3.1.3 4	Kaspersky Endpoint Security 11 Kaspersky Endpoint Security 11 для Windows Договор № ПР-00037842 от 4 декабря 2023 г. (ООО Прима АйТи)
6.3.1.3 5	ПАРУС-Бюджет 8.5.6.1 Платформа ПАРУС-Бюджет 8 Договор № 001-1 от 09.01.2017, Товарная накладная №1 от 23.01.2017
6.3.1.3	10-Strike File search pro Программа поиска файлов и документов в сети Лицензионный сертификат от 01.01.2011
6.3.1.3 7	10-Страйк Сканирование Сети Сканирование Сети - программа-сканер TCP-портов и IP-адресов Лицензионный сертификат от 01.01.2011
6.3.1.3 8	10-Страйк Инвентаризация Компьютеров Программа для учета ПК в сети предприятия Лицензионный сертификат от 01.01.2011
6.3.1.3 9	Open SuSe Linux Операционная система Open Source GNU/Linux Программное обеспечение по лицензии GNU GPL

6.3.1.4	MySQL Server Community СУБД MySQL Программное обеспечение по лицензии GNU GPL
6.3.1.4 1	Сервер администрирования Kaspersky Security Center Сервер администрирования Kaspersky Security Center Договор № ПР-00030672 от 01.12.2020 (ООО Прима АйТи)
6.3.1.4 2	УМКК «Телекоммуникации и сети» Учебно-методический компьютерный комплекс Диполь С00001 Номер лицензии: 20030400000000000033
6.3.1.4 3	УМКК «Коммутаторы локальных сетей» Учебно-методический компьютерный комплекс Диполь С00001 Номер лицензии: 20030400000000000033
6.3.1.4 4	УМКК «Электротехника и электроника» Учебно-методический компьютерный комплекс Диполь С00001 Номер лицензии: 20030400000000000033
6.3.1.4 5	УМКК «Информационные системы в экономике» Учебно-методический компьютерный комплекс Диполь С00001 Номер лицензии: 20030400000000000033
6.3.1.4 6	УМКК «Корпоративные информационные системы» Учебно-методический компьютерный комплекс Диполь С00001 Номер лицензии: 20030400000000000033
6.3.1.4 7	УМКК "Моделирование данных» Учебно-методический компьютерный комплекс Диполь С00001 Номер лицензии: 20030400000000000033
6.3.1.4 8	УМКК "Объектно-ориентированные технологии» Учебно-методический компьютерный комплекс Диполь С00001 Номер лицензии: 20030400000000000033
6.3.1.4 9	УМКК «Информационные технологии» Учебно-методический компьютерный комплекс Диполь С00001 Номер лицензии: 20030400000000000033
6.3.1.5 0	УМКК «Управление базами данных» Учебно-методический компьютерный комплекс Диполь С00001 Номер лицензии: 20030400000000000033
6.3.1.5 1	УМКК «Сетевые информационные технологии» Учебно-методический компьютерный комплекс Диполь С00001 Номер лицензии: 20030400000000000033
6.3.1.5 2	УМКК «Теоретические основы информатики» Учебно-методический компьютерный комплекс Диполь С00001 Номер лицензии: 20030400000000000033
6.3.1.5 3	УМКК "Основы алгоритмизации и программирования» Учебно-методический компьютерный комплекс Диполь С00001 Номер лицензии: 20030400000000000033
6.3.1.5	Apache HTTP Server Apache HTTP - веб-сервер Программное обеспечение по лицензии GNU GPL
6.3.1.5	Etxt Antiplagiat Проверка уникальности от сервиса Антиплагиат eTXT Freeware
6.3.1.5	Ramus Educational Case-средство для моделирования Программное обеспечение по лицензии GNU GPL
6.3.2. Перечень профессиональных баз данных и информационных справочных систем	
6.3.2.1	Консультант Плюс http://www.consultant.ru
6.3.2.2	РОССТАНДАРТ Федеральное агентство по техническому регулированию и метрологии https://www.gost.ru/portal/gost/
6.3.2.3	Кодекс – Профессиональные справочные системы https://kodeks.ru

7. МТО (оборудование и технические средства обучения)

Ауд	Наименование	ПО	Оснащение
Читальный зал	Информационно-библиотечный центр (помещение для самостоятельной работы обучающихся)	7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++ Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS Visio Pro 2016 Visual Studio Code Blender Gimp Maxima IntelliJ IDEA PyCharm Community Edition Adobe Reader DC MS Office Standart 2007 Windows 10 Pro	Стол - 20 шт., стул - 20 шт., рабочее место сотрудника - 2 шт., персональный компьютер с выходом в интернет и обеспечением доступа в электронную информационно-образовательную среду академии – 17 шт., multifunctional device – 2 шт.
208	Лаборатория Интеллектуальные системы и технологии	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox	Стол - 10 шт., стул - 21 шт., рабочее место преподавателя - 1 шт., персональных компьютеров с выходом в интернет - 20 шт., доска учебная – 1 шт., multifunctional device – 1 шт., мультимедийный проектор – 1 шт.,

	(Research Laboratory of Intelligent Systems and Technologies)	LibreOffice LibreCAD Inkscape Notepad++. Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox StarUML V1 PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclipse Adobe Reader DC Diptrace Embarcadero RAD Studio XE8 Arduino Software (IDE) NetBeans IDE ZEAL ARIS Express Archimate Klite Mega Codec Pack Ramus Educational Micro-Cap Evaluation gvSIG Desktop Python	проекционный экран – 1 шт., междисциплинарная лабораторная станция NI ELVIS II и ПО Circuit Design Suit - 1 шт, соответствующее программное обеспечение
114a	Компьютерный класс	Windows 10 Pro RUS 7-Zip Яндекс Браузер Mozilla Firefox LibreOffice LibreCAD Inkscape Notepad++. 1С:Предприятие 8. Комплект Kaspersky Endpoint Security MS Access 2016 MS Project Pro 2016 MS SQL Server 2019 MS SQL Server Management Studio 18.8 MS Visio Pro 2016 MS Visual Studio Community Edition Visual Studio Code Blender Gimp Maxima Oracle VM VirtualBox PostgreSQL IntelliJ IDEA PyCharm Community Edition Eclipse Adobe Reader DC NetBeans IDE ZEAL Klite Mega Codec Pack	Стол - 20 шт., стул - 22 шт., рабочее место преподавателя – 1 шт., персональный компьютер с выходом в интернет - 21 шт., доска учебная – 1 шт., многофункциональное устройство – 1 шт., мультимедийный проектор – 1 шт., проекционный экран – 1 шт., интерактивная доска WR-84A10 с проектором ViewSonic PS501X - 1 шт., соответствующее программное обеспечение

MS Office Standart 2010

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

Формой осуществления и развития науки является научное исследование, т. е. изучение с помощью научных методов явлений и процессов, анализа влияния на них различных факторов, а также, изучение взаимодействия между явлениями, с целью получения убедительно доказанных и полезных для науки и практики решений с максимальным эффектом.

Цель научного исследования – определение конкретного объекта и всестороннее, достоверное изучение его структуры, характеристик, связей на основе разработанных в науке принципов и методов познания, а также получение полезных для деятельности человека результатов, внедрение в производство с дальнейшим эффектом.

Основой разработки каждого научного исследования является методология, т. е. совокупность методов, способов, приемов и их определенная последовательность, принятая при разработ

-ке научного исследования. В конечном счете, методология – это схема, план решения поставленной научно-исследовательской задачи.

Процесс научно - исследовательской работы состоит из следующих основных этапов:

1. Выбор темы и обоснование ее актуальности.
2. Составление библиографии, ознакомление с законодательными актами, нормативными документами и другими источниками, относящимися к теме проекта (работы).
3. Разработка алгоритма исследования, формирование требований к исходным данным, выбор методов и инструментальных средств анализа.
4. Сбор фактического материала в статистических органах, на предприятиях различных форм собственности, в рыночных структурах и других организациях.
5. Обработка и анализ полученной информации с применением современных методов финансового и хозяйственного анализа, математико-статистических методов.
6. Формулировка выводов и выработка рекомендаций.
7. Оформление работы (проекта) в соответствии с установленными требованиями.

При выборе темы работы (проекта) полезно также принять во внимание следующие фак-торы:

- личный научный и практический интерес студента;
- возможность продолжения исследований, проведенных в процессе выполнения научно-исследовательской работы (проекта) по другим дисциплинам и иным научным работам;
- наличие оригинальных творческих идей;
- опыт публичных выступлений, докладов, участия в конференциях, семинарах;
- научную направленность кафедры и т.д.

9. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ОБУЧАЮЩИМСЯ ПО ВЫПОЛНЕНИЮ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Самостоятельная работа обучающихся в ходе семестра является важной составной частью учебного процесса и необходима для закрепления и углубления знаний, полученных в период сессии на лекциях, практических и интерактивных занятиях, а также для индивидуального изучения дисциплины в соответствии с программой и рекомендованной литературой.

Самостоятельная работа выполняется в виде подготовки домашнего задания или сообщения по отдельным вопросам, написание и защита научно-исследовательского проекта.

Контроль качества выполнения самостоятельной (домашней) работы может осуществляться с помощью устного опроса на лекциях или практических занятиях, обсуждения подготовленных научно-исследовательских проектов, проведения тестирования. Устные формы контроля помогут оценить владение обучающимися жанрами научной речи (дискуссия, диспут, сообщение, доклад и др.), в которых раскрывается умение обучающихся передать нужную информацию, грамотно использовать языковые средства, а также ораторские приемы для контакта с аудиторией.

Письменные работы позволяют оценить владение источниками, научным стилем изложения, для которого характерны: логичность, точность терминологии, обобщенность и отвлеченность, насыщенность фактической информацией.