

СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Факультет
Кафедра

Юридический
Теории и истории государства и права

Рабочая программа дисциплины (модуля)

дисциплина

Информационная безопасность в публично-правовой сфере

Блок Б1, вариативная часть, Б1.В.ДВ.05.02

цикл дисциплины и его часть (базовая, вариативная, дисциплина по выбору)

Направление

40.03.01

код

Юриспруденция

наименование направления

Программа

Государственно-правовой

Форма обучения

Очная

Для поступивших на обучение в
2019 г.

Разработчик (составитель)

к.и.н., доцент

Алешин П. Н.

ученая степень, должность, ФИО

Стерлитамак 2022

| | |
|---|-----------|
| 1. Перечень планируемых результатов обучения по дисциплине (модулю) | 3 |
| 1.1. Перечень планируемых результатов освоения образовательной программы | 3 |
| 1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы . | 3 |
| 2. Место дисциплины (модуля) в структуре образовательной программы | 4 |
| 3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся | 5 |
| 4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий..... | 5 |
| 4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах) | 5 |
| 4.2. Содержание дисциплины, структурированное по разделам (темам) | 6 |
| 5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю)..... | 10 |
| 6. Учебно-методическое и информационное обеспечение дисциплины (модуля) | 14 |
| 6.1. Перечень учебной литературы, необходимой для освоения дисциплины | 14 |
| 6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем | 15 |

1. Перечень планируемых результатов обучения по дисциплине (модулю)

1.1. Перечень планируемых результатов освоения образовательной программы

Выпускник, освоивший программу высшего образования, в рамках изучаемой дисциплины, должен обладать компетенциями, соответствующими видам профессиональной деятельности, на которые ориентирована программа:

| |
|---|
| Владением основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) |
| Способностью работать с информацией в глобальных компьютерных сетях (ОК-4) |
| Способностью обеспечивать соблюдение законодательства Российской Федерации субъектами права (ПК-3) |

1.2. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

| Формируемая компетенция (с указанием кода) | Этапы формирования компетенции | Планируемые результаты обучения по дисциплине (модулю) |
|--|---|--|
| Способностью обеспечивать соблюдение законодательства Российской Федерации субъектами права (ПК-3) | 1 этап: Знания | Обучающийся должен знать: основные нормативные правовые документы в области обеспечения информационной безопасности и защиты информации, а также нормативные методические документы ФСБ, ФСТЭК в данной области |
| | 2 этап: Умения | Обучающийся должен уметь: составлять и правильно оформлять деловую и служебную документацию, разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации; организовывать профилактическую работу с сотрудниками, имеющими доступ к информации ограниченного доступа |
| | 3 этап: Владения (навыки / опыт деятельности) | Обучающийся должен владеть: навыком работы с нормативными правовыми актами, навыками определения направлений и видов защиты информации с учетом характера информации и задач по ее защите. |
| Способностью работать с информацией в глобальных компьютерных сетях (ОК-4) | 1 этап: Знания | Обучающийся должен знать: виды информации, распространение которой запрещается или ограничивается в силу вреда, которое распространение этой информации наносит законным интересам и нравам субъектов информационных отношений; социально значимые проблемы и процессы в |

| | | |
|---|---|---|
| | | кибернетическом пространстве |
| | 2 этап: Умения | Обучающийся должен уметь: применять отечественные и зарубежные стандарты в области информационной безопасности с целью обоснования проектирования, разработки и оценки защищенности информации |
| | 3 этап: Владения (навыки / опыт деятельности) | Обучающийся должен владеть: профессиональной терминологией, навыками анализа информационных угроз в публично-правовой сфере |
| Владением основными методами, способами и средствами получения, хранения, переработки информации, навыками работы с компьютером как средством управления информацией (ОК-3) | 1 этап: Знания | Обучающийся должен знать основные методы хранения, обработки и защиты информации, ее правовой режим |
| | 2 этап: Умения | Обучающийся должен уметь: классифицировать информацию по режиму доступа, видам и типам; определять уровень достоверности источников информации и давать ей критическую оценку |
| | 3 этап: Владения (навыки / опыт деятельности) | Обучающийся должен владеть: навыками использования электронных средств обработки, использования и переработки информации в целях обеспечения информационной безопасности в публично-правовой сфере |

2. Место дисциплины (модуля) в структуре образовательной программы

Дисциплина реализуется в рамках вариативной части и относится к дисциплинам по выбору.

Для освоения дисциплины необходимы компетенции, сформированные в рамках изучения следующих дисциплин: Информационные технологии в деятельности органах публичной власти.

Последующие дисциплины - Земельное право, Предпринимательское право, Правовые институты информационного права, Правовые основы деятельности Федеральной службы судебных приставов, Правовые основы разрешительной деятельности, Конституционно-правовые основы охраны здоровья граждан РФ, Таможенное право.

Параллельно изучаемая дисциплина – Административное право, Экологическое право.

К изучению дисциплины «Информационная безопасность в публично-правовой сфере», обучающийся должен:

Знать сущность и содержание основных правовых понятий, категорий, институтов; сущность, содержание основных понятий действующего законодательства;

Уметь анализировать нормативные правовые акты на основе их всестороннего изучения; анализировать юридические факты и возникающие в связи с ними правоотношения;

Владеть навыками анализа различных правовых явлений, юридических фактов, правовых норм и правовых отношений, являющихся объектами профессиональной деятельности.

Дисциплина изучается на 2 курсе в 4 семестре

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических или астрономических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость (объем) дисциплины составляет 3 зач. ед., 108 акад. ч.

| Объем дисциплины | Всего часов |
|--|----------------------|
| | Очная форма обучения |
| Общая трудоемкость дисциплины | 108 |
| Учебных часов на контактную работу с преподавателем: | |
| лекций | 18 |
| практических (семинарских) | 22 |
| другие формы контактной работы (ФКР) | 0,2 |
| Учебных часов на контроль (включая часы подготовки): | |
| зачет | |
| Учебных часов на самостоятельную работу обучающихся (СР) | 67,8 |

| Формы контроля | Семестры |
|----------------|----------|
| зачет | 4 |

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1. Разделы дисциплины и трудоемкость по видам учебных занятий (в академических часах)

| № п/п | Наименование раздела / темы дисциплины | Виды учебных занятий, включая самостоятельную работу обучающихся и трудоемкость (в часах) | | | | СР |
|----------|---|---|-----------|----------|-------------|----|
| | | Контактная работа с преподавателем | | | СР | |
| | | Лек | Пр/Сем | Лаб | | |
| 2 | Система защиты информации: структурная и функциональная часть | 10 | 12 | 0 | 36,8 | |
| 2.4 | Ответственность за правонарушения в информационной сфере | 4 | 4 | 0 | 9 | |
| 1 | Понятие, организация и правовые основы обеспечения информационной безопасности в публично-правовой сфере | 8 | 10 | 0 | 31 | |
| 1.1 | Теоретические и вопросы организационного вопросы обеспечения информационной безопасности | 2 | 2 | 0 | 7 | |
| 1.2 | Правовые основы информационной безопасности | 4 | 2 | 0 | 6 | |
| 1.3 | Система организационно-правового обеспечения информационной безопасности. | 2 | 2 | 0 | 6 | |

| | | | | | |
|-----|---|-----------|-----------|----------|-------------|
| 1.4 | Информационные системы и технологии в государственном управлении | 0 | 2 | 0 | 6 |
| 1.5 | Государственные автоматизированные информационные системы и обеспечение информационной безопасности | 0 | 2 | 0 | 6 |
| 2.2 | Актуальные проблемы правового и организационного обеспечения информационной безопасности | 2 | 4 | 0 | 9 |
| 2.3 | Особенности организационно-правового обеспечения защиты информационных систем | 2 | 2 | 0 | 9 |
| 2.1 | Правовые режимы обеспечения безопасности информации ограниченного доступа | 2 | 2 | 0 | 9,8 |
| | Итого | 18 | 22 | 0 | 67,8 |

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

| № | Наименование раздела / темы дисциплины | Содержание |
|----------|---|---|
| 2 | Система защиты информации: структурная и функциональная часть | |
| 2.4 | Ответственность за правонарушения в информационной сфере | Система правовой ответственности за утечку информации и утрату носителей информации. Виды и условия применения правовых норм гражданско-правовой, административной и дисциплинарной ответственности за разглашение защищаемой информации и невыполнение правил ее защиты. Понятие и классификация компьютерных преступлений. Уголовно-правовая и криминалистическая характеристика. Организационно-правовые основы деятельности подразделений защиты государственной тайны. Место структурного подразделения защиты государственной тайны в системе защиты государственной и служебной тайны. |
| 1 | Понятие, организация и правовые основы обеспечения информационной безопасности в публично-правовой сфере | |
| 1.1 | Теоретические и организационные вопросы обеспечения информационной безопасности | Угрозы информационной безопасности и условия правового обеспечения их нейтрализации. Понятие об информационном объекте и его элементах. Информационная безопасность как предмет реализации мер правового и организационного обеспечения. Содержание мер организационного и правового обеспечения информационной безопасности. Объекты и методы обеспечения информационной безопасности. Концептуальные и правовые основы формирования системы обеспечения информационной безопасности. Система правовых норм в сфере обеспечения информационной безопасности. Социальные нормы в обеспечении информационной |

| | | |
|-----|--|---|
| | | безопасности: моральные, правовые, политические, эстетические, корпоративные. Техничко-правовые нормы и роль технического регулирования в обеспечении информационной безопасности. |
| 1.2 | Правовые основы информационной безопасности | Право и его роль в регулировании комплекса отношений в информационной сфере, объекты и субъекты правоотношений. Отрасли права, обеспечивающие законность в интересах информационной безопасности. Структура и направленность правовых мер обеспечения информационной безопасности. Информационная сфера как сфера обращения информации и правового регулирования. Юридические особенности и свойства информации. Правовая классификация информационных ресурсов, продуктов и услуг. Информационные отношения. Система и нормы информационного права. Правонарушения в информационной сфере. |
| 1.3 | Система организационно-правового обеспечения информационной безопасности. | Политика безопасности. Требования действующих международных стандартов по вопросам менеджмента информационной безопасности. Принципы организационного обеспечения информационной безопасности. Силы и средства обеспечения информационной безопасности. Функции органов управления и подразделения защиты информации в системе обеспечения информационной безопасности. Роль внешних контролирующих органов в системе обеспечения информационной безопасности |
| 2.2 | Актуальные проблемы правового и организационного обеспечения информационной безопасности | Противодействие экстремистской деятельности в информационной сфере. Защита детей от информации, причиняющей вред их здоровью и развитию .Правовые проблемы обеспечения информационной безопасности в сети Интернет |
| 2.3 | Особенности организационно-правового обеспечения защиты информационных систем | Особенности организационно-правового обеспечения процессов создания автоматизированных систем в защищенном исполнении Особенности организационно-правового обеспечения защиты информационных систем в сфере судопроизводства Практика разработки и реализации политики информационной безопасности корпоративных информационных систем |
| 2.1 | Правовые режимы обеспечения безопасности информации ограниченного доступа | Понятие и защита государственной тайны в системе защиты информации. Действующие нормативные правовые акты, нормативно-методические и методические документы в системе защиты государственной и коммерческой тайны. Принципы защиты. Отнесение сведений к коммерческой, |

| | |
|--|--|
| | <p>служебной и профессиональной тайнам. Перечень сведений, составляющих коммерческую тайну. Сведения, которые не могут составлять государственную и коммерческую тайну. Права обладателя информации, составляющей коммерческую тайну.</p> <p>Степени и грифы секретности. Засекречивание и рассекречивание. Основания и порядок доступа к конфиденциальной информации. Государственное лицензирование деятельности, связанное с защитой информации</p> |
|--|--|

Курс практических/семинарских занятий

| № | Наименование раздела / темы дисциплины | Содержание |
|----------|---|--|
| 2 | Система защиты информации: структурная и функциональная часть | |
| 2.4 | Ответственность за правонарушения в информационной сфере | <ol style="list-style-type: none"> 1. Система правовой ответственности за утечку информации и утрату носителей информации. 2. Виды и условия применения правовых норм гражданско-правовой, административной и дисциплинарной ответственности за разглашение защищаемой информации и невыполнение правил ее защиты. 3. Понятие и классификация компьютерных преступлений. Уголовно-правовая и криминалистическая характеристика. 4. Организационно-правовые основы деятельности подразделений защиты государственной тайны. |
| 1 | Понятие, организация и правовые основы обеспечения информационной безопасности в публично-правовой сфере | |
| 1.1 | Теоретические и организационные вопросы обеспечения информационной безопасности | <ol style="list-style-type: none"> 1. Современное информационное противоборство и обеспечение информационной безопасности 2. Информационная безопасность в системе национальной безопасности Российской Федерации 3. Базовые принципы обеспечения информационной безопасности 4. Правовое регулирование информационной безопасности в системе российского информационного права |
| 1.2 | Правовые основы информационной безопасности | <ol style="list-style-type: none"> 1. Правовая основа обеспечения информационной безопасности в России. 2. Регламентирование вопросов защиты информации в ведомственных нормативных актах. |

| | | |
|-----|---|---|
| | | <ul style="list-style-type: none"> 3. Правовое регулирование информационной безопасности публично-правовой сфере 4. Способы незаконного получения защищаемой информации |
| 1.3 | Система организационно-правового обеспечения информационной безопасности. | <ul style="list-style-type: none"> 1. Система защиты информации. Структурная и функциональная часть защиты информации. 2. Государственная система организационно-правового обеспечения информационной безопасности. 3. Основные категории и функции органов защиты информации. 4. Основные формы организации работ по защите информации 5. Причины и условия утечки защищаемой информации. |
| 1.4 | Информационные системы и технологии в государственном управлении | <ul style="list-style-type: none"> 1. Сущность информационных систем и технологий государственного и муниципального управления 2. Электронное государство (электронные государственные услуги) 3. Реестр государственных информационных систем 4. Государственные автоматизированные системы 5. Требования к государственным информационным системам |
| 1.5 | Государственные автоматизированные информационные системы и обеспечение информационной безопасности | <ul style="list-style-type: none"> 1. ГАС «Выборы». 2. Автоматизированные информационные системы Министерства юстиции РФ. 3. ГАС «Правосудие» 4. ГАС «Управление» |
| 2.2 | Актуальные проблемы правового и организационного обеспечения информационной безопасности | <ul style="list-style-type: none"> 1. Противодействие экстремистской деятельности в информационной сфере 2. Защита детей от информации, причиняющей вред их здоровью и развитию 3. Правовые проблемы обеспечения информационной безопасности в сети Интернет |
| 2.3 | Особенности организационно-правового обеспечения защиты информационных систем | <ul style="list-style-type: none"> 1. Особенности организационно-правового обеспечения процессов создания автоматизированных систем в защищенном исполнении 2. Особенности организационно-правового обеспечения защиты информационных систем в сфере судопроизводства 3. Практика разработки и реализации политики информационной безопасности |

| | | |
|-----|---|---|
| | | информационных систем государственных организаций и учреждений |
| 2.1 | Правовые режимы обеспечения безопасности информации ограниченного доступа | <ol style="list-style-type: none"> 1. Ограничение доступа к информации в целях защиты интересов личности, общества и государства 2. Правовые режимы тайн в системе организационного и правового обеспечения безопасности информации ограниченного доступа 3. Правовой режим защиты государственной тайны 4. Правовой режим обеспечения безопасности персональных данных 5. Актуальные вопросы режима служебной тайны |

5. Учебно-методическое обеспечение для самостоятельной работы обучающихся по дисциплине (модулю)

Внеаудиторная самостоятельная работа студентов – это планируемая учебная, учебно-исследовательская, научно-исследовательская работа студентов, выполняемая во внеаудиторное время по заданию и при методическом руководстве преподавателя, при этом носящая сугубо индивидуальный характер. По курсу **«Информационная безопасность в публично-правовой сфере»** самостоятельная работа обучаемых предполагает выработку навыков изучения первоисточников и другой литературы во внеаудиторное время.

Целью самостоятельной работы студентов является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа студентов способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Тема 1.1. Теоретические и вопросы организационного вопросы обеспечения информационной безопасности

1. Раскройте основное содержание понятия «обеспечение информационной безопасности» человека на территории Российской Федерации; коммерческой и некоммерческой организаций; федерального органа исполнительной власти.

2. Определите функциональную направленность правового режима информационной безопасности для сети связи общего пользования.

3. Что такое «информационное противоборство» и каковы причины его возникновения?

4. Как проявляется информационное противоборство в информационно-технической области?

5. Какие известны правовые средства противодействия вредоносному использованию информационных технологий государствами?

6. Какие правовые средства противодействия использованию системы массовой информации для вмешательства во внутренние дела других государств вам известны?

Тема 1.2. Правовые основы информационной безопасности

1. Проанализируйте сходство и различие определений понятия персональных данных, закрепленных в Федеральном законе «О персональных данных», Основных положениях Организации по экономическому сотрудничеству и развитию (ОЭСР) о защите неприкосновенности частной жизни и международных обменов персональных данных, Конвенции Совета Европы о защите физических лиц в отношении автоматизированной обработки данных личного характера (ЕТ8 № 108), Директиве 95/46/ЕС Европейского парламента и Совета Европейского союза о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных, проанализируйте содержание понятия персональных данных в Федеральном законе «О персональных данных», Основных положениях Организации по экономическому сотрудничеству и развитию (ОЭСР) о защите неприкосновенности частной жизни и международных обменов персональных данных, Конвенции Совета Европы о защите физических лиц в отношении автоматизированной обработки данных личного характера (ЕТЗ № 108), Директиве 95/46/ЕС Европейского парламента и Совета Европейского союза о защите прав частных лиц применительно к обработке персональных данных и о свободном движении таких данных.

Тема 1.3. Система организационно-правового обеспечения информационной безопасности.

1. Каковы основные угрозы информационной безопасности в сфере информационно-телекоммуникационных систем?

2. Как организуется оценка безопасности технологий обработки, хранения и передачи информации в государственных АС.

8. На основе каких нормативных актов и служебных документов осуществляется контроль и регистрация действий пользователей и событий информационной безопасности в АС?

Сформулируйте понятие «мобильные угрозы». Проанализируйте основные тенденции информационной преступности.

9. Изучите экспертные оценки состояния информационной преступности с помощью официального сайта лаборатории Касперского.

10. Проанализировать угрозу — использование ИКТ в преступных целях.

Тема 1.4. Информационные системы и технологии в государственном управлении

1. Когда было положено начало автоматизации функциональных задач в государственном и региональном управлении?

2. . Какие автоматизированные системы в настоящее время применяются для информационного обслуживания органов федерального управления?

3. Дайте сравнительную характеристику действующим в федеральном и региональном управлении автоматизированным системам и ситуационным центрам. Каковы их функциональные, организационные и технологические особенности?

4. Перечислите важнейшие теоретические и организационно-технологические принципы создания и функционирования информационной системы и информационной технологии муниципального управления.

5. Какие требования предъявляются к локальным вычислительным сетям города и автоматизированному рабочему месту специалистов для качественного информационного обслуживания управленческих процессов?

6. Дайте понятие государственных информационных ресурсов.
7. Какие функции выполняют «интернет-порталы» госуслуг?

Тема 1.5. Государственные автоматизированные информационные системы и обеспечение информационной безопасности

1. Каковы основные угрозы информационной безопасности в сфере общегосударственных информационно-телекоммуникационных систем?
2. Раскройте особенности организационно-правового обеспечения управления защитой общегосударственных информационно-телекоммуникационных систем.
3. Каковы правовые нормы и обязательные требования по защите информации в АС?
4. Перечислите основные требования по созданию защищенной АС.

Тема 2.1. Правовые режимы обеспечения безопасности информации ограниченного доступа

1. Раскройте содержание права на доступ к информации и его ограничение в целях защиты интересов личности, общества и государства.
2. Раскройте содержание понятия тайны.
3. Какие права и обязанности установлены в законодательстве для обладателя информации, составляющей государственную тайну?
5. В чем состоят проблемы правового режима служебной тайны?
6. Раскройте понятие и виды персональных данных.
7. Охарактеризуйте принципы и условия обработки персональных данных.
8. Какие права и обязанности установлены для оператора при обработке персональных данных?
9. Какой орган осуществляет контроль и надзор за обработкой персональных данных?

Тема 2.2. Актуальные проблемы правового и организационного обеспечения информационной безопасности

1. Каков порядок ограничения доступа к информационным ресурсам в сети Интернет, распространяющих экстремистские материалы?
2. Какая ответственность предусмотрена за распространение экстремистских материалов?
4. Какая информация запрещена к распространению среди детей?
5. Какая информация ограничена к распространению среди детей?
6. Какие требования касающиеся защиты детей от информации, причиняющей вред их здоровью и развитию, закреплены в законодательстве о средствах массовой информации?
7. Перечислите требования к обороту информационной продукции, содержащей информацию, запрещенную или ограниченную к распространению среди детей.

Тема 2.3. Особенности организационно-правового обеспечения защиты информационных систем

1. Сопоставьте актуальные задачи формирования единого информационного пространства органов государственной власти с задачами обеспечения информационной безопасности Российской Федерации.
2. Разъясните положения Доктрины информационной безопасности и основных нормативных правовых актов РФ об особенностях обеспечения информационной безопасности в сфере судебной и правоохранительной деятельности.
3. Каковы особенности обеспечения информационной безопасности АС в условиях модернизации информационной инфраструктуры судебной системы России?

Тема 2.4. Ответственность за правонарушения в информационной сфере

1. Какие существуют виды юридической ответственности за правонарушения в информационной сфере?
2. Чем отличается дисциплинарная, административная и уголовная ответственность за правонарушения в информационной сфере?
3. Как можно классифицировать преступления в информационной сфере?
4. Дайте общую характеристику отечественного законодательства в сфере информационных преступлений.
5. Назовите особенности ответственности субъектов сети Интернет за преступления в информационной сфере.
6. Определите основные тенденции информационной преступности

Темы рефератов по дисциплине «Информационная безопасность в публично-правовой сфере».

1. Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства).
2. Правовое обеспечение информационной безопасности публично-правовой сфере
3. Виды защищаемой информации.
4. Угрозы информационной безопасности в публично-правовой сфере
5. Проблемы региональной информационной безопасности.
6. Информационное оружие, его классификация и возможности.
7. Методы нарушения конфиденциальности (целостности, доступности)
8. информации.
9. Правовые (организационно-технические, экономические) методы обеспечения информационной безопасности
10. Компьютерная система как объект информационной безопасности.
11. Обеспечение информационной безопасности компьютерных систем.
12. Субъекты информационного противоборства.
13. Цели информационного противоборства.
14. Составные части и методы информационного противоборства.
15. Причины, виды, каналы утечки и искажения информации.
16. Основные направления обеспечения информационной безопасности объектов информационной сферы государства в условиях информационной войны.
17. Правовые, организационно-технические и экономические методы обеспечения информационной безопасности.
18. Модели, стратегии и системы обеспечения информационной безопасности.
19. Критерии и классы защищенности средств вычислительной техники и

20. автоматизированных информационных систем

Основные требования, предъявляемые к реферату:

1. Выбор темы

Тему реферата студент выбирает, основываясь на специально разработанную «Тематику рефератов».

2. Работа над рефератом

Работу над рефератом нужно начинать с подборки и изучения монографической литературы, статей в философских, социологических и экономических журналах и других источников по избранной теме.

Составив план работы, студент должен комплексно изучить каждый вопрос и систематически изложить его в тексте реферата. Ценность работы повышается, если студент использовал возможно более широкий круг литературы по данной теме и умело систематизировал собранный материал.

3. Требования к оформлению

Объем реферата должен быть примерно 20-22 страниц печатного текста, который набирается на компьютере через 1,5 интервала 14-м шрифтом.

На второй странице, после титульного листа располагается «план» работы или «содержание». В него должны входить введение, главы и параграфы основной части, заключение, список использованной литературы

Реферат следует оформлять аккуратно, оставляя поля для замечаний рецензента. Текст реферата должен быть разделен на подзаголовки, выделяемые в соответствии с вопросами плана.

Приводимые в тексте цитаты, а также статистические данные необходимо сопровождать примечаниями – ссылками на источники, из которых они взяты, с указанием автора, названия работы, места, года издания, тома, страницы. Ссылки должны располагаться на соответствующем листе реферата.

6. Учебно-методическое и информационное обеспечение дисциплины (модуля)

6.1. Перечень учебной литературы, необходимой для освоения дисциплины

Основная учебная литература:

1. Куняев, Н. Н. Правовое обеспечение национальных интересов Российской Федерации в информационной сфере : монография / Н. Н. Куняев. — Москва : Логос, 2020. — 348 с. — ISBN 978-5-98704-513-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/163040>
2. Бегларян, М. Е. Понятия, технологии и процессы для юридической информационной сферы : учебное пособие / М. Е. Бегларян, В. Г. Мелоян, И. А. Терентьев. — Москва : РГУП, 2020. — 112 с. — ISBN 978-5-93916-778-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/172949>
3. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI:

<https://doi.org/10.29039/1761-6>. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1189326>

4. Дровалева, Л. С. Информационные технологии в юридической деятельности : учебное пособие / Л. С. Дровалева. — Москва : РГУП, 2020. — 152 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/172959>

Дополнительная учебная литература:

1. Осавелюк, Е. А. Информационная безопасность государства и общества в контексте деятельности СМИ : монография / Е. А. Осавелюк. — 2-е изд., стер. — Санкт-Петербург : Лань, 2020. — 92 с. — ISBN 978-5-8114-5001-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/130481>
2. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1844364>
3. Милкина, Е. В. Информационное право : учебно-методическое пособие / Е. В. Милкина. — Москва : РТУ МИРЭА, 2019. — 99 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/171458>
4. Бабаш, А. В. История защиты информации в зарубежных странах : учебное пособие / А.В. Бабаш, Д.А. Ларин. — Москва : РИОР : ИНФРА-М, 2021. — 284 с. — (Высшее образование). — DOI: <https://doi.org/10.12737/15090>. - ISBN 978-5-369-01844-6. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1215133>
5. Азизов, Р. Ф. Правовое регулирование в интернет-пространстве: история, теория, компаративистика : монография / Р. Ф. Азизов. — Санкт-Петербург : Алетейя, 2020. — 266 с. — ISBN 978-5-00165-087-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/141755>
6. Нестеров, С. А. Основы информационной безопасности : учебник для вузов / С. А. Нестеров. — Санкт-Петербург : Лань, 2021. — 324 с. — ISBN 978-5-8114-6738-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/165837>
7. Бабаш, А. В. Моделирование системы защиты информации. Практикум : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 3-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 320 с. + Доп. материалы [Электронный ресурс]. — (Высшее образование). — DOI: <https://doi.org/10.29039/01848-4>. - ISBN 978-5-369-01848-4. - Текст : электронный. - URL: <https://znanium.com/catalog/product/1232287>

6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем

| № п/п | Наименование документа с указанием реквизитов |
|--------------|--|
|--------------|--|