

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сыров Игорь Анатольевич
Должность: Директор
Дата подписания: 24.06.2022 16:59:40
Уникальный программный ключ:
b683afe664d7e9f64175886cf9626a196149ad56

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

Факультет Юридический
Кафедра Теории и истории государства и права

Рабочая программа дисциплины (модуля)

дисциплина ***Б1.О.08 Информационная безопасность в правоохранительной сфере***

обязательная часть

Направление

40.04.01
код

Юриспруденция
наименование направления

Программа

Юрист в правоохранительной деятельности

Форма обучения

Заочная

Для поступивших на обучение в
2021 г.

Разработчик (составитель)
к.и.н., доцент
Алешин П. Н.
ученая степень, должность, ФИО

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций	3
2. Цели и 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	4
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).....	8
Тема 10. Особенности организационно-правового обеспечения защиты информационных систем в сфере судопроизводства	11
Тема 11. Противодействие экстремистской деятельности в информационной сфере	12
6. Учебно-методическое и информационное обеспечение дисциплины (модуля)	14
6.1. Перечень учебной литературы, необходимой для освоения дисциплины (модуля)	14
6.2. Перечень электронных библиотечных систем, современных профессиональных баз данных и информационных справочных систем	15

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)
<p>ОПК-7. Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности</p>	<p>ОПК-7.1. Знает основные методы и средства хранения, поиска, систематизации, обработки, передачи и защиты информации; состав, функции и конкретные возможности профессионально-ориентированных справочных информационно-правовых и информационно-поисковых систем, правила защиты конфиденциальной информации</p>	<p>Обучающийся должен знать методы аналитической работы в подготовке правового обеспечения информационной безопасности правоохранительной сфере; основные нормативные правовые документы в области обеспечения информационной безопасности и защиты информации</p>
	<p>ОПК-7.2. Умеет получать юридически значимую информацию из профессионально-ориентированных справочных информационно-правовых и информационно-поисковых систем; решать задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий с учетом требований информационной безопасности</p>	<p>Обучающийся должен уметь применять нормы информационного права в правоохранительной сфере; составлять и правильно оформлять деловую и служебную документацию; разрабатывать нормативно-методические материалы по регламентации системы организационной защиты информации, определять виды и формы информации, подверженной угрозам, формировать комплекс мер по информационной безопасности с учетом его правовой обоснованности</p>
	<p>ОПК-7.3. Владеет навыками работы с информационно-</p>	<p>Обучающийся должен владеть навыками работы с автоматизированными</p>

	поисковыми и информационно-справочными системами и базами данных, используемыми в профессиональной деятельности, с учетом основных требований информационной безопасности	информационно-справочными и информационно-поисковыми системами; навыками работы с базами данных; навыками анализа информационных угроз в правоохранительной сфере навыками организации
--	---	--

2. Цели и место дисциплины (модуля) в структуре образовательной программы

Цели изучения дисциплины:

Дисциплина реализуется в рамках обязательной части.

Цель дисциплины - подготовить магистрантов к пониманию и решению информационно-аналитических задач в правоохранительной сфере, более глубокому усвоению сведений о правоохранительных органах и механизме их функционирования.

Дисциплина предназначена для формирования теоретических знаний и практических навыков в области владения технологиями обработки, хранения, передачи и приема массивов профессиональной информации в различных сферах деятельности практика-юриста в современном мире; приобретение навыков работы в справочно-правовых системах.

К изучению дисциплины «Информационная безопасность в правоохранительной 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 1 курсе в 1, 2 семестрах

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 108 акад. ч.

Объем дисциплины	Всего часов
	Заочная форма обучения
Общая трудоемкость дисциплины	108
Учебных часов на контактную работу с преподавателем:	
лекций	6
практических (семинарских)	10
другие формы контактной работы (ФКР)	0,2

Учебных часов на контроль (включая часы подготовки):	3,8
зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	88

Формы контроля	Семестры
зачет	2

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		
1	Раздел 1.	4	2	0	44	
1.3	Источники угроз защищаемой информации.	2	0	0	5	
1.2	История и современные направления развития информационной безопасности.	0	0	0	15	
1.1	Основы правового регулирования отношений в информационной сфере	2	0	0	5	
2.3	Компьютерные технологии в информационно-аналитическом обеспечении прокуратуры города (района)	0	2	0	7	
2.2	Информационные технологии и обеспечение безопасности в правоохранительной деятельности	2	0	0	5	
2	Раздел 2.	2	8	0	44	
1.6	Система организационно-правового обеспечения информационной безопасности.	0	0	0	0	
1.5	Правовые основы защиты тайны и персональных данных	0	2	0	7	
1.4	Общая характеристика способов незаконного получения защищаемой информации	0	0	0	12	
2.4	Особенности организационно-правового обеспечения защиты информационных систем в сфере судопроизводства	0	2	0	5	
2.5	Противодействие экстремистской деятельности в информационной сфере	0	2	0	7	
2.6	Ответственность за правонарушения в информационной сфере	0	2	0	0	

2.1	Применение информационных технологий в целях обеспечения законности, правопорядка, безопасности личности, общества и государств	0	0	0	12
2.7	Особенности предупреждения преступлений в информационной сфере и обеспечения информационной безопасности	0	0	0	8
	Итого	6	10	0	88

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Раздел 1.	
2.3	Компьютерные технологии в информационно-аналитическом обеспечении прокуратуры города (района)	<ol style="list-style-type: none"> 1. Многоуровневая территориально-распределенная информационная структура, охватывающая инфраструктуру Генеральной прокуратуры Российской Федерации и прокуратуры субъектов Российской Федерации. 2. Информационная система обеспечения надзора за исполнением законов. Приказ Генерального прокурора Российской Федерации от 18.11.2004 № 25-10. 3. Использование средств правового мониторинга ресурсов сети Интернет в районной прокуратуре. Информационные порталы прокуратур субъектов Российской Федерации. 4. Организация доступа к информационно-аналитическим ресурсам из прокуратур городов и районов. 5. Системы информационного обеспечения функциональной деятельности в районной прокуратуре.
2	Раздел 2.	
1.5	Правовые основы защиты тайны и персональных данных	<ol style="list-style-type: none"> 1. Понятие и защита государственной и коммерческой тайны в системе защиты информации. 2. Действующие нормативные правовые акты, нормативно-методические и методические документы в системе защиты государственной и коммерческой тайны. 3. Принципы защиты. Отнесение сведений к коммерческой, служебной и профессиональной тайнам. 4. Перечень сведений, составляющих государственную тайну. Сведения, которые не могут составлять государственную и коммерческую тайну.

		<p>5. Степени и грифы секретности. Засекречивание и рассекречивание. Основания и порядок доступа к конфиденциальной информации. Государственное лицензирование деятельности, связанное с защитой информации.</p>
2.4	Особенности организационно-правового обеспечения защиты информационных систем в сфере судопроизводства	<p>1..Информационная инфраструктура судопроизводства 2.Реализация принципа единства судебной систем в информационно-телекоммуникационной сфере и формирование единого информационного пространства в области судопроизводства. 3. Процессуальная специфика защиты электронных документов в сфере судопроизводства 4. Функция информационного обеспечения обвинения и юридической защиты в уголовном процессе 5. Проблемы исключения фальсификаций доказательств, представляемых в электронном виде</p>
2.5	Противодействие экстремистской деятельности в информационной сфере	<p>1.Понятие экстремистской деятельности в информационной сфере 2.Порядок признания информационных материалов экстремистскими. Федеральный список экстремистских материалов 3. Административная и уголовная ответственность за правонарушения экстремистской направленности</p>
2.6	Ответственность за правонарушения в информационной сфере	<p>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. 4. Уголовно-правовая и криминалистическая характеристика. 5. Организационно-правовые основы деятельности подразделений защиты государственной тайны.</p>

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	Раздел 1.	

1.3	Источники угроз защищаемой информации.	Классификация и содержание возможных угроз информации в правоохранительной сфере. Причины и условия утечки защищаемой информации. Разглашение, раскрытие и распространение защищаемой информации. Способы незаконного получения защищаемой информации.
1.1	Основы правового регулирования отношений в информационной сфере	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.
2.2	Информационные технологии и обеспечение безопасности в правоохранительной деятельности	Цели и задачи внедрения информационных технологий в правоохранительной деятельности. Информационные технологии в деятельности органов внутренних дел. Автоматизированные информационные системы федеральных служб, подведомственных Министерству юстиции Российской Федерации. Структура и состав автоматизированных информационных систем. Основные потребители информации, информационных ресурсов, информационных продуктов, информационных систем правоохранительной органов.
2	Раздел 2.	

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

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

Целью самостоятельной работы является овладение фундаментальными знаниями, профессиональными умениями и навыками деятельности по профилю, опытом творческой, исследовательской деятельности. Самостоятельная работа магистрантов

способствует развитию самостоятельности, ответственности и организованности, творческого подхода к решению проблем учебного и профессионального уровня.

Тематика самостоятельной работы

Тема 1. Назначение и структура правового обеспечения информационной безопасности

Тема 3. Основные законодательные акты и правовые нормы в сфере обеспечения информационной безопасности

1. Проведите сравнение функциональной направленности режима обеспечения информационной безопасности Российской Федерации и режима обеспечения безопасности киберпространства США.
2. Определите основные правовые средства противодействия использованию глобальной информационной инфраструктуры и социальных сетей для вмешательства во внутренние дела других государств. В процессе выполнения работы проведите анализ политических и нормативных правовых актов, определяющих субъектов, уполномоченных устанавливать режим информационной безопасности, задачи по противодействию угрозам безопасности, функциональную направленность использования правовых средств и организационных мероприятий, составляющих соответствующие правовые и организационные режимы информационной безопасности.

Тема 1. Основы правового регулирования отношений в информационной сфере

1. Определите функциональную направленность режимов информационной безопасности выделенных преподавателем объектов безопасности. В процессе выполнения работы проведите анализ политических и нормативных правовых актов, определяющих субъектов, уполномоченных устанавливать режим информационной безопасности, задачи по противодействию угрозам безопасности, функциональную направленность использования правовых средств и организационных мероприятий, составляющих соответствующие правовые и организационные режимы информационной безопасности.
2. Сформулируйте позицию по вопросам, выделенным в тексте раздела для самостоятельного обдумывания. Подберите необходимую литературу, обосновывающую позицию по обсуждаемым вопросам.

Тема 2. История и современные направления развития информационной безопасности

1. Сформулируйте функциональную направленность организационного режима информационной безопасности публичной библиотеки.
2. Объясните влияние положений основных документов Всемирной встречи на высшем уровне по информационному обществу для функциональной направленности режима информационной безопасности Российской Федерации.
3. Какие известны правовые средства противодействия вредоносному использованию информационных технологий государствами?

Тема 3. Источники угроз защищаемой информации

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.
3. На основе каких нормативных актов и служебных документов осуществляется контроль и регистрация действий пользователей и событий информационной безопасности в АС?
4. Сформулируйте понятие «мобильные угрозы». Проанализируйте основные тенденции информационной преступности.
5. Изучите экспертные оценки состояния информационной преступности с помощью официального сайта лаборатории Касперского.
6. Проанализировать угрозу – использование ИКТ в преступных целях.

Тема 4. Общая характеристика способов незаконного получения защищаемой информации

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. Какими организациями обеспечивается международное сотрудничество в борьбе с трансграничной преступностью в информационной сфере и каковы актуальные проблемы в этой области?
6. Назовите особенности ответственности субъектов сети Интернет за преступления в информационной сфере.
7. Определите основные тенденции информационной преступности

Тема 5. Правовые основы защиты тайны и персональных данных

1. Проанализируйте существующие подходы к определению служебной тайны. Обоснуйте свою точку зрения на указанную проблему.
2. Раскройте понятие и виды персональных данных.
3. Охарактеризуйте принципы и условия обработки персональных данных.
4. Какие права и обязанности установлены для оператора при обработке персональных данных?
5. Какой орган осуществляет контроль и надзор за обработкой персональных данных?
6. Перечислите полномочия государственного органа, осуществляющего контроль и надзор за обработкой персональных данных.
7. Какая ответственность предусмотрена за нарушение положений законодательства о персональных данных?

Тема 6. Система организационно-правового обеспечения информационной безопасности

1. Как проявляется информационное противоборство в области идеологии?

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

Тема 7. Применение информационных технологий в целях обеспечения законности, правопорядка, безопасности личности, общества и государств

1. Раскройте основное содержание понятия «обеспечение информационной безопасности» человека на территории Российской Федерации;
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?

Тема 8. Информационные технологии и обеспечение безопасности в правоохранительной деятельности

1. Проанализируйте содержание правового режима безопасности видов информации. В процессе выполнения работы ознакомьтесь с нормативными правовыми актами, определяющими субъектов, уполномоченных устанавливать режим информационной безопасности, задачи по противодействию угрозам безопасности, функциональную направленность использования правовых средств, составляющих соответствующий правовой режим безопасности информации.
2. Какими организациями обеспечивается международное сотрудничество в борьбе с трансграничной преступностью в информационной сфере и каковы актуальные проблемы в этой области?
3. Назовите особенности ответственности субъектов сети Интернет за преступления в информационной сфере.

Тема 9. Компьютерные технологии в информационно-аналитическом обеспечении прокуратуры города (района)

1. Информационно-аналитическое обеспечение прокуратуры как составная часть проекта создания «Информационной системы обеспечения надзора за исполнением законов в органах прокуратуры»
2. Автоматизированная система АИК «Надзор» в районной прокуратуре
3. Использование АРМ «Статистика» в районной прокуратуре
4. Автоматизированное рабочее место государственного обвинителя.
5. Программный комплекс АИСС «НОРД»

Тема 10. Особенности организационно-правового обеспечения защиты информационных систем в сфере судопроизводства

1. Проанализируйте особенности обеспечения информационной безопасности в сфере автоматизированного судопроизводства. Чем они обусловлены?
2. Какие комплексы средств автоматизации обеспечивают защиту информации ограниченного доступа в судебной системе на федеральном уровне?

3. Как организовано формирование единого информационного пространства федеральных судов общей юрисдикции и мировых судей в Судебном департаменте при Верховном Суде РФ?

4. Раскройте сущность реализации принципа единства судебной системы в информационно-телекоммуникационной сфере и обеспечения понятийного единства в области обеспечения информационной безопасности судопроизводства.

Тема 11. Противодействие экстремистской деятельности в информационной сфере

1. Приведите определение понятие экстремистских материалов, закрепленное в законодательстве.
2. Сформулируйте основные положения российского законодательства о противодействии распространению экстремистских материалов.
3. Каков порядок ограничения доступа к информационным ресурсам в сети Интернет, распространяющих экстремистские материалы?
4. Какая ответственность предусмотрена за распространение экстремистских материалов?
5. Перечислите правовые основания мониторинга и блокирования доступа к информации в сети Интернет.

Тема 12. 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.

Тема 13. Особенности предупреждения преступлений в информационной сфере и обеспечения информационной безопасности

1. Политика безопасности. Требования действующих международных стандартов по вопросам менеджмента информационной безопасности. Принципы организационного обеспечения информационной безопасности.
2. Силы и средства обеспечения информационной безопасности. Функции органов управления и подразделения защиты информации в системе обеспечения информационной безопасности.
3. Роль внешних контролирующих органов в системе обеспечения информационной безопасности.
4. Возможности специализированных организаций по формированию требований к информационной безопасности корпорации и контролю эффективности их выполнения.
5. Направления и методы работы с персоналом, обладающим конфиденциальной информацией. Обязанности администрации по созданию надлежащих условий персоналу для работы с конфиденциальной информацией.

Темы рефератов по самостоятельной работе

1. Место и роль информационной безопасности в различных сферах жизнедеятельности личности (общества, государства).
2. Правовое обеспечение информационной безопасности правоохранительной сфере.
3. Виды защищаемой информации.
4. Угрозы информационной безопасности в правоохранительной 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
21. Компьютерная система как объект информационной безопасности.
22. Общая характеристика методов и средств защиты информации.
23. Организационно-правовые, технические и криптографические методы
24. обеспечения информационной безопасности.
25. Программно-аппаратные средства обеспечения информационной безопасности.

Основные требования, предъявляемые к реферату:

1. Выбор темы

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

3. Требования к оформлению

Объём 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 (модуля)

Основная учебная литература:

1. 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>
2. Мальцев, В. А. Правовое обеспечение информационной безопасности в Российской Федерации : учебно-методическое пособие / В. А. Мальцев. — Воронеж : ВГУ, 2017. — 40 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/154824>
3. Арзуманян, А. Б. Международные стандарты правовой защиты информации и информационных технологий : учебное пособие / А. Б. Арзуманян. — Ростов-на-Дону : ЮФУ, 2020. — 140 с. — ISBN 978-5-9275-3546-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/170355>

Дополнительная учебная литература:

1. Ворожевич, А. С. Современные информационные технологии и право : монография / А. С. Ворожевич, Е. В. Зайченко, Е. Е. Кирсанова ; под редакцией Е. Б. Лаутс. — Москва : СТАТУТ, 2019. — 288 с. — ISBN 978-5-8354-1578-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/130674>
2. Волков, С. Н. Социальные и философские проблемы информационного общества : учебник для вузов / С. Н. Волков. — Санкт-Петербург : Лань, 2021. — 112 с. — ISBN 978-5-8114-6605-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/162370>
3. 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>

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

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