

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Сыров Игорь Анатольевич
Должность: Директор
Дата подписания: 24.06.2022 16:43:43
Уникальный программный ключ:
b683afe664d7e9f64175886cf9626a196149ad56

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

Факультет
Кафедра

Юридический
Теории и истории государства и права

Аннотация рабочей программы 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.

Стерлитамак 2022

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.	