СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет ***Юридический***
Кафедра ***Теории и истории государства и права***

Аннотация рабочей программы 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	***Юриспруденция***
код	наименование направления

Программа

Государственно-правовой

Форма обучения

Очно-заочная

Для поступивших на обучение в
2019 г.

Стерлитамак 2023

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)
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
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 рас-пространение этой информации наносит законным интересам и нравам субъектов информационных от-ношений; 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	Обучающийся должен владеть:

	(навыки / опыт деятельности)	профессиональной терминологией, навыками анализа информационных угроз в публично-правовой сфере
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.

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 4 курсе в 7 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**
	Очно-заочная обучения
Общая трудоемкость дисциплины	108
Учебных часов на контактную работу с преподавателем:	
лекций	8
практических (семинарских)	10
другие формы контактной работы (ФКР)	0,2
Учебных часов на контроль (включая часы подготовки):	
зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	89,8

Формы контроля	**Семестры**
зачет	7

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)**			
		Контактная работа с преподавателем			**СР**
		Лек	**Пр/Сем**	**Лаб**	
1	**Понятие, организация и правовые основы обеспечения информационной безопасности в публично-правовой сфере**	**4**	**6**	**0**	**49,8**
1.1	Теоретические и вопросы организационного вопросы обеспечения информационной безопасности	2	2	0	9,8
1.2	Правовые основы информационной безопасности	2	0	0	10
1.3	Система организационно-правового обеспечения информационной безопасности.	0	2	0	10
1.4	Информационные системы и технологии в государственном	0	0	0	10

	управлении				
1.5	Государственные автоматизированные информационные системы и обеспечение информационной безопасности	0	2	0	10
2	**Система защиты информации: структурная и функциональная часть**	**4**	**4**	**0**	**40**
2.1	Правовые режимы обеспечения безопасности информации ограниченного доступа	2	2	0	10
2.2	Актуальные проблемы правового и организационного обеспечения информационной безопасности	0	2	0	10
2.3	Особенности организационно-правового обеспечения защиты информационных систем	2	0	0	10
2.4	Ответственность за правонарушения в информационной сфере	0	0	0	10
	Итого	**8**	**10**	**0**	**89,8**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Понятие, организация и правовые основы обеспечения информационной безопасности в публично-правовой сфере**	
1.1	Теоретические и вопросы организационного 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. Технико-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.
2	**Система защиты информации: структурная и функциональная часть**	
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, служебной и профессиональной тайнам. Перечень сведений, составляющих коммерческую тайну. Сведения, которые не могут составлять государственную и коммерческую тайну. Права обладателя информации, составляющей коммерческую тайну. Степени и грифы секретности. Засекречивание и рассекречивание. Основания и порядок доступа к конфиденциальной информации. Государственное лицензирование деятельности, связанное с защитой информации
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

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**Понятие, организация и правовые основы обеспечения информационной безопасности в публично-правовой сфере**	
1.1	Теоретические и вопросы организационного вопросы обеспечения информационной безопасности	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

1.3	Система организационно-правового обеспечения информационной безопасности.	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.
1.5	Государственные автоматизированные информационные системы и обеспечение информационной безопасности	1. ГАС «Выборы». 2. Автоматизированные информационные системы Министерства юстиции РФ. 3. ГАС «Правосудие» 4. ГАС «Управление»
2	**Система защиты информации: структурная и функциональная часть**	
2.1	Правовые режимы обеспечения безопасности информации ограниченного доступа	1. Ограничение доступа к информации в целях защиты интересов личности, общества и государства 2. Правовые режимы тайн в системе организационного и правового обеспечение безопасности информации ограниченного доступа 3. Правовой режим защиты государственной тайны 4. Правовой режим обеспечения безопасности персональных данных 5. Актуальные вопросы режима служебной тайны
2.2	Актуальные проблемы правового и организационного обеспечения информационной безопасности	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