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 ***Б1.О.08 Информационные технологии и информационная безопасность в органах публичной власти***

обязательная часть

Направление

40.04.01	***Юриспруденция***
код	наименование направления

Программа

Антикоррупционная деятельность

Форма обучения

Очная

Для поступивших на обучение в
2022 г.

Стерлитамак 2023

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)
ОПК-7. Способен применять информационные технологии и использовать правовые базы данных для решения задач профессиональной деятельности с учетом требований информационной безопасности	ОПК-7.1. Знает методы и программные инструменты поиска, сбора, обработки и анализа информации о коррупционных рисках, коррупционном поведении и его последствиях. функции и конкретные возможности профессионально-ориентированных справочных информационно-правовых и информационно-поисковых систем, правила защиты конфиденциальной информации	Обучающийся должен: знать информационные технологии, используемые в профессиональной деятельности юриста, основные нормативные правовые документы в области обеспечения информационной безопасности и защиты информации, способы и приемы правового обеспечения информационной безопасности и защиты конфиденциальной информации, формы электронного взаимодействия органов государственной и муниципальной власти с организациями и гражданами, правила обеспечения информационной безопасности в цифровой среде
	ОПК-7.2. Умеет работать с источниками информации, цифровыми инструментами и средами с целью поиска и обработки информации, необходимой для реализации отдельных задач антикоррупционной деятельности; использовать методы коллективной работы в цифровой среде, в том числе, с интеллектуальными устройствами, для сбора, обработки и анализа данных при решении отдельных задач антикоррупционной деятельности; использовать методы визуализации данных и результатов• их анализа с учетом особенностей осуществления антикоррупционной	Обучающийся должен: уметь пользоваться прикладными программами для обработки текстов и таблиц, правовыми базами данных, разрабатывать и реализовывать систему мер, направленных на правовое обеспечение информационной безопасности включая защиту конфиденциальной информации

	деятельности; интерпретировать данные и результаты их обработки с учетом особенностей осуществления антикоррупционной деятельности	
	ОПК-7.3. Владеет навыками работы с информационно-поисковыми и информационно-справочными системами и базами данных, используемыми антикоррупционной деятельности с учетом основных требований информационной безопасности	Обучающийся должен: владеть навыками работы с автоматизированными информационно-справочными и информационно-поисковыми системами; навыками работы с базами данных; навыками работы с нормативными правовыми актами, навыками определения направлений и видов защиты информации с учетом характера информации и задач по ее защите навыками анализа информационных угроз в органах государственной и муниципальной власти

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 антикоррупционной деятельности, более глубокому усвоению сведений о правоохранительных органах и механизме их функционирования в сфере противодействия коррупции.

Изучение учебной дисциплины «Информационные технологии и информационная безопасность в органах публичной власти» предполагает наличие у магистранта базовых познаний в области информационного права. К изучению дисциплины «Информационная безопасность в органах публичной власти», 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 2 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	12
практических (семинарских)	16
другие формы контактной работы (ФКР)	0,2
Учебных часов на контроль (включая часы подготовки):	
зачет	
Учебных часов на самостоятельную работу обучающихся (СР)	79,8

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)			
		Контактная работа с преподавателем			СР
		Лек	Пр/Сем	Лаб	
1	**раздел 1**	**6**	**4**	**0**	**30,8**
1.1	Информационная безопасность: понятие, сущность, виды	2	0	0	7
1.2	Правовое регулирование в сфере информационной безопасности	2	2	0	7
1.3	Источники угроз информационной безопасности и общая характеристика способов незаконного получения защищаемой информации	2	0	0	9,8
1.4	Понятие и виды субъектов информационной безопасности	0	2	0	7
2	**раздел 2**	**6**	**12**	**0**	**49**
2.1	Система органов государственной власти, регулирующих информационную безопасность	2	0	0	7
2.2	Единое информационное пространство органов государственной власти	2	0	0	7
2.3	Информационные технологии в государственном и муниципальном	0	4	0	7

	управлении, обеспечение информационной безопасности				
2.4	Защита и обработка документов ограниченного доступа	2	0	0	7
2.5	Особенности защиты информации в системах электронного документооборота	0	4	0	7
2.6	Информационные технологии в правотворческой деятельности	0	2	0	7
2.7	Информационные технологии в правоприменительной деятельности	0	2	0	7
	Итого	**12**	**16**	**0**	**79,8**

4.2. Содержание дисциплины, структурированное по разделам (темам)

Курс практических/семинарских занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**раздел 1**	
1.2	Правовое регулирование в сфере информационной безопасности	1.Международные стандарты по информационной безопасности 2.Конституционные основы информационной безопасности в Российской Федерации. 3.Система законодательства, регулирующего общественные отношения, возникающие в процессах применения информационных технологий. 4. Законодательное регулирование реализации права граждан, органов государственной власти, органов местного самоуправления и организаций на доступ к информации. 5. Концепция формирования в Российской Федерации электронного правительства.
1.4	Понятие и виды субъектов информационной безопасности	1.Понятие субъекта информационной безопасности. Виды субъектов информационной безопасности 2.Российская Федерация как субъект информационной безопасности. 3.Субъекты РФ и муниципальные образования субъекты информационной безопасности. 4.Граждане и другие физические лица как субъекты информационной безопасности. 5.Права граждан в информационной сфере. Право на доступ к информации. Право на защиту персонифицированной информации.
2	**раздел 2**	
2.3	Информационные технологии в государственном и муниципальном управлении, обеспечение информационной безопасности	1. Стратегия развития информационного общества в Российской Федерации. 2. Основные направления внедрения информационных технологий в правовой

		сфере. 3. Структура государственных информационных ресурсов Российской Федерации. 4. Информационные технологии в деятельности органов и учреждений Министерства юстиции Российской Федерации, подведомственных ему федеральных служб. 5. Автоматизированные правовые информационные системы, базы и банки данных. 6.Применение справочных правовых систем и иных информационных технологий в правотворческой деятельности.. 7.Государственная автоматизированная система «Управление», государственная автоматизированная система «Выборы»: общая характеристика и обеспечение их информационной безопасности. 8.Основные потребители информации, информационных ресурсов, информационных продуктов, информационных систем правоохранительной органов.
2.5	Особенности защиты информации в системах электронного документооборота	1.Понятие электронного документооборота. Угрозы безопасности электронной информации. 2Требования к обеспечению безопасности систем электронного документооборота. 3Организация доступа к ограниченным массивам электронных документов, базам данных. 4.Возможности систем электронного документооборота с точки зрения защиты от угроз (рисков) безопасности информации.
2.6	Информационные технологии в правотворческой деятельности	1. Использование информационных технологий в правотворческой деятельности. Назначение, функции и задачи информатизации правотворческой деятельности. 2. Правотворческий процесс. 3. Алгоритм разработки проекта нормативного правового акта. 4. Применение справочных правовых систем и иных информационных технологий в правотворческой деятельности. 5. Автоматизированные информационные системы Федерального Собрания Российской Федерации. 6. Автоматизированные информационные системы Министерства юстиции Российской Федерации.

2.7	Информационные технологии в правоприменительной деятельности	1. Использование информационных технологий в судебной деятельности. 2. Задачи внедрения информационных технологий в правоприменительной деятельности. 3. Государственная автоматизированная система «Правосудие». 4. Государственная автоматизированная система «Выборы». 5. Автоматизированные информационные системы федеральных служб, подведомственных Министерству юстиции Российской Федерации. 6. Информатизация таможенных, налоговых органов, Пенсионного фонда Российской Федерации.

Курс лекционных занятий

№	Наименование раздела / темы дисциплины	Содержание
1	**раздел 1**	
1.1	Информационная безопасность: понятие, сущность, виды	Понятие информационной безопасности, основные задачи и методы ее обеспечения. Национальные интересы РФ в информационной сфере и их обеспечение. Угрозы информационной безопасности. Государственная политика в сфере информационной безопасности. Комплекс мер, реализованный в Российской Федерации, по совершенствованию обеспечения ее информационной безопасности. Влияние современных условий политического и социально-экономического развития страны на обеспечение информационной безопасности. Основные задачи по обеспечению информационной безопасности.
1.2	Правовое регулирование в сфере информационной безопасности	Конституционные основы использования информационных технологий в Российской Федерации.Система законодательства, регулирующего общественные отношения, возникающие в процессах применения информационных технологий.Законодательное регулирование реализации права граждан, органов государственной власти, органов местного самоуправления и организаций на доступ к информации. Электронные источники опубликования актов.Концепция формирования в Российской Федерации электронного правительства.
1.3	Источники угроз информационной безопасности и общая характеристика способов	Понятие «источник угрозы информационной безопасности» и его виды. Правовое регулирование средств массовой информации. Способы незаконного получения защищаемых сведений, особенности.

	незаконного получения защищаемой информации	Похищение документов, содержащих защищаемые сведения. Незаконное получение конфиденциальной информации путем перехвата информации, циркулирующей в технических средствах и помещениях. Незаконное завладение конфиденциальной информацией, содержащейся в средствах вычислительной техники. Защита от информационного воздействия. Информационная война. Промышленный шпионаж.
2	**раздел 2**	
2.1	Система органов государственной власти, регулирующих информационную безопасность	Государственное управление в информационной сфере. Система и полномочия органов государственной власти, обеспечивающих право доступа к информации. Система и компетенция органов, обеспечивающих охрану государственной тайны. Компетенция органов государственной власти по обеспечению правового режима конфиденциальной информации. Взаимодействие органов местного самоуправления и органов государственной власти в условиях информационного общества. Информационное государство
2.2	Единое информационное пространство органов государственной власти	Система межведомственного электронного взаимодействия Информационные системы межведомственного взаимодействия по предоставлению государственных услуг Обеспечение доступности государственных услуг для граждан и организаций Автоматизации управления отдельными сферами государственной деятельности Предоставление комплексных государственных и муниципальных услуг на базе многофункциональных центров. Автоматизированные места специалистов в сфере государственного и муниципального управления. Технологии телекоммуникаций. Экономическая эффективность территориальных информационных систем управления. Автоматизированные информационные системы в государственном и муниципальном управлении и обеспечение их информационной безопасности
2.4	Защита и обработка документов ограниченного доступа	Понятие о защите и обработке документов ограниченного доступа. Понятие государственной тайны и ограниченной информации. Виды информационных ресурсов по категориям доступа. Понятия «утрата» и «разглашение» ограниченной информации. Классификация информационных ресурсов по категориям доступа. Комплекс организационных мер по охране ограниченной информации. Организация ограниченного делопроизводства Задачи экспертной комиссии по защите ограниченной информации.

		Документирование ограниченной информации. Определение состава документируемой ограниченной информации. Перечень издаваемых документов ограниченного доступа. Требования к разработке системы доступа к ограниченным документам. Контроль наличия кофиденциальных документов. Проведение внутренних расследований по фактам утраты (разглашения) документов ограниченного доступа.