Приложение № 4
к образовательной программе высшего образования – программе магистратуры
по направлению подготовки 09.04.01 Информатика и вычислительная техника
(направленность (профиль) «Разработка и управление
критической информационной инфраструктурой»)

**АВТОНОМНАЯ НЕКОММЕРЧЕСКАЯ ОБРАЗОВАТЕЛЬНАЯ ОРГАНИЗАЦИЯ ВЫСШЕГО ОБРАЗОВАНИЯ «НАУЧНО-ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ «СИРИУС»
(АНОО ВО «УНИВЕРСИТЕТ «СИРИУС»)**

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ
Сертификат: 7835bcdac1c89a3da835a18f6045494f3f404337
Владелец: Некрасова Людмила Андреевна
Действителен: с 08.07.2026 до 08.07.2027

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

«Правовое обеспечение информационной безопасности»

1. Трудоемкость дисциплины (модуля): 3 з.е.

2. Место дисциплины (модуля) в учебном плане:

Обязательная часть «Профессиональной подготовки» в рамках Блока 1. Дисциплины (модули), реализуется в 1 семестре.

3. Цель дисциплины (модуля): формирование навыков работы с правовыми актами в области информационной безопасности, а также понимания юридических аспектов защиты информации, ответственности и правовых норм при обработке, передаче и хранении информации.

4. Задачи дисциплины (модуля):

– сформировать представление о законодательной базе РФ в области информационной безопасности, правовых режимах государственной, коммерческой тайны и персональных данных;

– обеспечить владение нормативно-правовыми актами, регулирующими создание, эксплуатацию и защиту объектов критической информационной инфраструктуры;

– научить применять правовые механизмы и организационные меры для обеспечения информационной безопасности при разработке и внедрении программных и аппаратных продуктов.

5. Перечень разделов (тем) дисциплины (модуля) и их краткое содержание:

Наименование раздела (темы) дисциплины (модуля)	**Краткое содержание**
Раздел 1. Законодательная и нормативная базы по информационной безопасности.	Понятие тайны. Основные виды тайн. Международная нормативная база. Законы РФ. Кодексы, включающие в себя правовые вопросы защиты охраняемой законом тайны.
Раздел 2. Основные понятия и практика применения Закона о государственной тайне.	Закон РФ «О государственной тайне». Основные понятия. Принципы, порядок засекречивания и рассекречивания сведений, составляющих государственную тайну. Допуск и доступ к сведениям, составляющих государственную тайну. Лицензирование деятельности предприятий в вопросах государственной тайны.
Раздел 3. Коммерческая тайна на предприятии. Правовые вопросы защиты персональных данных	Коммерческая тайна. Основные понятия. Основные положения Закона о коммерческой тайне. Режим коммерческой тайны. Предоставление сведений, составляющих коммерческую тайну. Правоприменение положений Закона о коммерческой тайне на предприятии. Нормативная документация в области защиты персональных данных. Правоприменение положений нормативных документов в условиях предприятия. Вопросы защиты персональных данных в судебном порядке.

Наименование раздела (темы) дисциплины (модуля)	Краткое содержание
Раздел 4. Организационные вопросы защиты информации на предприятии	Предприятие как объект защиты. Основные виды угроз информационной безопасности. Концепция информационной безопасности. Модель угроз информационной безопасности. Политика информационной безопасности предприятия. Государственные стандарты в области информационной безопасности.
Раздел 5. Мировая практика в области защиты информации	Законы и нормативные акты о защите информации. Методы защиты информации от кибератак и утечек данных. Защита персональных данных. Юридическая ответственность за нарушение правил защиты информации. Влияние законодательства на развитие технологий в сфере информационной безопасности.
Раздел 6. Законодательная и нормативная база по критической информационной инфраструктуре	Законодательная база о критической информационной инфраструктуре. Определение критической информационной инфраструктуры и классификация объектов критической информационной инфраструктуры. Меры по защите критической информационной инфраструктуры от киберугроз. Роли и обязанности органов правительства и компаний в обеспечении безопасности критической информационной инфраструктуры. Сотрудничество между государственными и частными организациями для обеспечения безопасности критической информационной инфраструктуры.

6. Образовательные результаты освоения дисциплины (модуля):

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
ПК-8. Способен управлять проектированием объектов критической информационной инфраструктуры с учетом требований отрасли и индустрии	ИПК-8.1. Знает основы проектирования объектов критической инфраструктуры и информационных систем, методики обеспечения их безопасности, а также знает нормативно-правовую базу, регулирующую процесс разработки и внедрения программных и аппаратных продуктов
	ИПК-8.2. Умеет разрабатывать планы управления проектированием объектов

Код и наименование компетенции	Код и наименование индикатора достижения компетенции
	критической инфраструктуры с учетом их безопасности, координировать деятельность специалистов
	ИПК-8.3. Владеет методами анализа и управления процессами проектирования объектов критической информационной инфраструктуры с учетом требований отрасли, индустрии, а также норм законодательства в области разработки и внедрения программных и аппаратных продуктов