

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Ястребов Олег Александрович

Должность: Ректор

Дата подписания: 28.05.2025 12:23:30

Уникальный программный ключ:

ca953a0120d891083f939673078ef1a989dae18a

**Федеральное государственное автономное образовательное учреждение высшего образования**

**«Российский университет дружбы народов имени Патриса Лумумбы»**

**Факультет искусственного интеллекта**

(наименование основного учебного подразделения (ОУП)-разработчика ОП ВО)

## **РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

### **ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

(наименование дисциплины/модуля)

**Рекомендована МССН для направления подготовки/специальности:**

#### **10.03.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ**

(код и наименование направления подготовки/специальности)

**Освоение дисциплины ведется в рамках реализации основной профессиональной образовательной программы высшего образования (ОП ВО):**

#### **ОРГАНИЗАЦИЯ И ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ (ПО ОТРАСЛИ ИЛИ В СФЕРЕ ПРОФЕССИОНАЛЬНОЙ ДЕЯТЕЛЬНОСТИ)**

(наименование (профиль/специализация) ОП ВО)

**2025 г.**

## 1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Организационное и правовое обеспечение информационной безопасности» входит в программу бакалавриата «Организация и технологии защиты информации (по отрасли или в сфере профессиональной деятельности)» по направлению 10.03.01 «Информационная безопасность» и изучается в 4 семестре 2 курса. Дисциплину реализует Кафедра прикладного искусственного интеллекта. Дисциплина состоит из 2 разделов и 10 тем и направлена на изучение равовых аспектов защиты информации, организационных мер по обеспечению информационной безопасности, а также механизмов управления рисками в сфере информационных технологий. В рамках данной дисциплины студенты знакомятся с законодательными актами, регуливающими защиту информации, стандартами и нормами в области информационной безопасности, а также методиками разработки и внедрения политик и процедур по защите информации в организациях.

Целью освоения дисциплины является формирование у студентов комплекса знаний и навыков, необходимых для эффективного управления информационными ресурсами организации и обеспечения их правовой и организационной защиты.

## 2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Организационное и правовое обеспечение информационной безопасности» направлено на формирование у обучающихся следующих компетенций (части компетенций):

*Таблица 2.1. Перечень компетенций, формируемых у обучающихся при освоении дисциплины (результаты освоения дисциплины)*

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.2 В рамках поставленных задач определяет имеющиеся ресурсы, ограничения и действующие правовые нормы;
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты	ОПК-10.1 Знает методы и средства формирования политики информационной безопасности, организации и поддержания выполнения комплекса мер по обеспечению информационной безопасности, управления процессом их реализации на объекте защиты; ОПК-10.2 Принимает участие в формировании политики информационной безопасности, организации и поддержании выполнения комплекса мер по обеспечению информационной безопасности, управлении процессом их реализации на объекте защиты;
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК-5.1 Знает нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности; ОПК-5.2 Применяет нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности;
ОПК-6	Способен при решении профессиональных задач организовывать защиту	ОПК-6.1 Знает методы и средства организации защиты информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю	методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю; ОПК-6.2 При решении профессиональных задач организует защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю;
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК-8.1 Знает методы и средства подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;

### 3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Организационное и правовое обеспечение информационной безопасности» относится к обязательной части блока 1 «Дисциплины (модули)» образовательной программы высшего образования.

В рамках образовательной программы высшего образования обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Организационное и правовое обеспечение информационной безопасности».

*Таблица 3.1. Перечень компонентов ОП ВО, способствующих достижению запланированных результатов освоения дисциплины*

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
УК-2	Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	Правоведение;	Комплексное обеспечение защиты информации объекта информатизации; <i>Методы принятия решений**</i> ; <i>Теория систем и системный анализ**</i> ; Эксплуатационная практика; Преддипломная практика; Технологическая практика; Исследовательская практика;
ОПК-6	Способен при решении профессиональных задач организовывать защиту информации ограниченного доступа в соответствии с нормативными правовыми актами, нормативными и методическими документами Федеральной		Эксплуатационная практика; Технологическая практика; Защищенный документооборот; Комплексное обеспечение защиты информации объекта информатизации; Программно-аппаратные средства защиты информации;

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
	службы безопасности Российской Федерации, Федеральной службы по техническому и экспортному контролю		
ОПК-5	Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности		Эксплуатационная практика; Технологическая практика; Исследовательская практика; Защищенный документооборот; Комплексное обеспечение защиты информации объекта информатизации;
ОПК-8	Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	Информационные технологии; Основы информационной безопасности (введение в специальность);	Комплексное обеспечение защиты информации объекта информатизации; Исследовательская практика; Эксплуатационная практика; Технологическая практика;
ОПК-10	Способен в качестве технического специалиста принимать участие в формировании политики информационной безопасности, организовывать и поддерживать выполнение комплекса мер по обеспечению информационной безопасности, управлять процессом их реализации на объекте защиты		Защита информации от утечки по техническим каналам; Комплексное обеспечение защиты информации объекта информатизации; Эксплуатационная практика; Технологическая практика;
	Способен разрабатывать, внедрять и сопровождать комплекс мер по обеспечению безопасности объекта защиты с применением локальных нормативных актов и стандартов информационной безопасности		Эксплуатационная практика; Технологическая практика; Основы управления информационной безопасностью; Комплексное обеспечение защиты информации объекта информатизации; Аудит информационной безопасности; Защита информации от утечки по техническим каналам;

\* - заполняется в соответствии с матрицей компетенций и СУП ОП ВО

\*\* - элективные дисциплины /практики

#### 4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Организационное и правовое обеспечение информационной безопасности» составляет «5» зачетных единиц.

Таблица 4.1. Виды учебной работы по периодам освоения образовательной программы высшего образования для очной формы обучения.

Вид учебной работы	ВСЕГО, ак.ч.		Семестр(-ы)
			4
<i>Контактная работа, ак.ч.</i>	68		68
Лекции (ЛК)	34		34
Лабораторные работы (ЛР)	0		0
Практические/семинарские занятия (СЗ)	34		34
<i>Самостоятельная работа обучающихся, ак.ч.</i>	85		85
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	27		27
<b>Общая трудоемкость дисциплины</b>	<b>ак.ч.</b>	<b>180</b>	<b>180</b>
	<b>зач.ед.</b>	<b>5</b>	<b>5</b>

## 5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Таблица 5.1. Содержание дисциплины (модуля) по видам учебной работы

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
Раздел 1	Правовые основы информационной безопасности	1.1	Назначение и структура правового обеспечения информационной безопасности.	ЛК, СЗ
		1.2	Основы правового регулирования отношений в информационной сфере.	ЛК, СЗ
		1.3	Основные законодательные акты и правовые нормы в сфере обеспечения информационной безопасности.	ЛК, СЗ
		1.4	Правовые основы защиты тайны и персональных данных.	ЛК, СЗ
		1.5	Ответственность за правонарушения в информационной сфере.	ЛК, СЗ
		1.6	Правовая защита обладателей информации.	ЛК, СЗ
Раздел 2	Организационные основы информационной безопасности.	2.1	Содержание организационного обеспечения информационной безопасности.	ЛК, СЗ
		2.2	Организация внутриобъектового, пропускного режима и охраны предприятия.	ЛК, СЗ
		2.3	Обеспечение информационной безопасности предприятия при работе со СМИ и в рекламной деятельности.	ЛК, СЗ
		2.4	Организация аналитической работы по предупреждению утечки конфиденциальной информации.	ЛК, СЗ

\* - заполняется только по **ОЧНОЙ** форме обучения: ЛК – лекции; ЛР – лабораторные работы; СЗ – практические/семинарские занятия.

## 6. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Таблица 6.1. Материально-техническое обеспечение дисциплины

Тип аудитории	Оснащение аудитории	Специализированное учебное/лабораторное оборудование, ПО и материалы для освоения дисциплины (при необходимости)
Лекционная	Аудитория для проведения занятий лекционного типа, оснащенная комплектом специализированной мебели; доской (экраном) и техническими средствами мультимедиа презентаций.	
Семинарская	Аудитория для проведения занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебели и техническими средствами мультимедиа презентаций.	
Для самостоятельной работы	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и	

	консультаций), оснащенная комплектом специализированной мебели и компьютерами с доступом в ЭИОС.	
--	--	--

\* - аудитория для самостоятельной работы обучающихся указывается **ОБЯЗАТЕЛЬНО!**

## 7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

### *Основная литература:*

1. Окинавская хартия глобального информационного общества. 22 июля 2000 г.
2. Гражданский кодекс Российской Федерации. Часть IV.
3. Федеральный закон № 310-ФЗ «О безопасности», 26 декабря 2010 г.
4. «Стратегия национальной безопасности Российской Федерации до 2020 г.».
- Указ Президента РФ №537 от 12.05.2009
5. Доктрина информационной безопасности Российской Федерации (утв. Президентом РФ 9 сентября 2000 г. № Пр-1895).
6. Федеральный закон РФ «Об информации, информационных технологиях и о защите информации» от 27.07. 2006 г. № 149-ФЗ.
7. «О подписании Соглашения о сотрудничестве государств-участников СНГ в области обеспечения информационной безопасности». Расп. Пр. РФ от 28.05.2012 № 856-р «Собрание законодательства РФ», 04.06.2012, № 23, ст. 3058.
8. Федеральный закон № 5485-1 «О государственной тайне», 21 июля 1993 г. (с изм. от 6.10.97 г. и от 11.12.2011 г.), – М.: МВК по ЗГТ, 2011.
9. Федеральный закон № 98-ФЗ «О коммерческой тайне», 29 июля 2004 г.
10. Федеральный закон № 152-ФЗ «О персональных данных», 27 июля 2006 г.
11. Федеральный закон № 69-ФЗ «О пожарной безопасности».
12. Постановление правительства РФ «Об утверждении положения о порядке обращения со служебной информацией ограниченного распространения в ФОИВ» № 1233 от 03 ноября 1994 г. – М.: МВК по ЗГТ, 1998.
13. Постановление правительства РФ «Об утверждении правил отнесения сведений к различным степеням секретности» № 170 от 20 февраля 1995 г. – М.: МВК по ЗГТ, 1998.
14. Инструкция о порядке допуска должностных лиц и граждан РФ к государственной тайне. Постановление Правительства РФ от 6 февраля 2010 г. № 63
15. Международный стандарт ИСО/МЭК 27001. Первое издание 2005-10-15. Информационные технологии. Методы защиты. Системы менеджмента защиты информации.
16. ГОСТ Р ИСО/МЭК 15408-2002. Методы и средства обеспечения безопасности критерии оценки безопасности информационных технологий (КОБИТ). Части 1, 3-5.
17. ГОСТ Р ИСО/МЭК 17799-2005. Информационная технология. Практические правила управления информационной безопасностью.
18. «Об утверждении Типовой инструкции по делопроизводству в ФОИВ»: Пр. Федеральной архивной службы России от 27.11.2000 г. № 68.
19. Копылов В.А. Информационное право. – М., 2011. – М.: Юридические науки. – 247 с.
20. Рассолов И.М. Информационное право. Учебник. – М.: Норма: ИНФРА-М, 2010. – 352 с.

### *Дополнительная литература:*

1. Стрельцов А.А. Информационная безопасность Российской Федерации. – М.: Высшая школа, 2003.
2. Садердинов А.А. Информационная безопасность предприятия. Уч. пособие. – М.: Дашков и Ко, 2004.
3. Ярочкин В.И. Система безопасности фирмы. – М.: Ось-89, 2003.
4. Журавлев С.Ю. «Частная охрана». – М.: 1994.

*Ресурсы информационно-телекоммуникационной сети «Интернет»:*

1. ЭБС РУДН и сторонние ЭБС, к которым студенты университета имеют доступ на основании заключенных договоров

- Электронно-библиотечная система РУДН – ЭБС РУДН

<https://mega.rudn.ru/MegaPro/Web>

- ЭБС «Университетская библиотека онлайн» <http://www.biblioclub.ru>

- ЭБС Юрайт <http://www.biblio-online.ru>

- ЭБС «Консультант студента» [www.studentlibrary.ru](http://www.studentlibrary.ru)

- ЭБС «Знаниум» <https://znaniium.ru/>

2. Базы данных и поисковые системы

- Sage <https://journals.sagepub.com/>

- Springer Nature Link <https://link.springer.com/>

- Wiley Journal Database <https://onlinelibrary.wiley.com/>

- Научометрическая база данных Lens.org <https://www.lens.org>

*Учебно-методические материалы для самостоятельной работы обучающихся при освоении дисциплины/модуля\*:*

1. Курс лекций по дисциплине «Организационное и правовое обеспечение информационной безопасности».

\* - все учебно-методические материалы для самостоятельной работы обучающихся размещаются в соответствии с действующим порядком на странице дисциплины **в ТУИС!**

**РАЗРАБОТЧИК:**

\_\_\_\_\_

*Должность, БУП*

*Подпись*

*Фамилия И.О.*

**РУКОВОДИТЕЛЬ БУП:**

\_\_\_\_\_

Заведующий кафедрой

*Должность БУП*

\_\_\_\_\_

*Подпись*

\_\_\_\_\_

Подолько Павел  
Михайлович [М]  
заведующий кафедрой

*Фамилия И.О.*

**РУКОВОДИТЕЛЬ ОП ВО:**

\_\_\_\_\_

*Должность, БУП*

\_\_\_\_\_

*Подпись*

\_\_\_\_\_

*Фамилия И.О.*