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

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки/специальности:

10.04.01 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ
(код и наименование направления подготовки/специальности)

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

УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ
(наименование (профиль/специализация) ОП ВО)

2025 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Управление информационной безопасностью» входит в программу магистратуры «Управление информационной безопасностью» по направлению 10.04.01 «Информационная безопасность» и изучается в 3 семестре 2 курса. Дисциплину реализует Кафедра прикладного искусственного интеллекта. Дисциплина состоит из 7 разделов и 10 тем и направлена на изучение методов и средств управления информационной безопасностью (ИБ) в организации, а также изучение основных подходов к разработке, реализации, эксплуатации, анализу, сопровождению и совершенствованию систем управления информационной безопасностью (СУИБ) определенного объект

Целью освоения дисциплины является приобретение необходимого объема знаний и практических навыков по управлению информационной безопасностью, оценки рисков информационных ресурсов организации и аудита информационной безопасности, организации работы и разграничения полномочий персонала, ответственного за информационную безопасность; формирование представления о содержании процессов управления информационной безопасностью организации как результата внедрения системного подхода к решению задач обеспечения информационной безопасности

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Управление информационной безопасностью» 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 управлять проектом на всех этапах его жизненного цикла	УК-2.1 Анализирует план-график реализации проекта в целом и выбирает оптимальный способ решения поставленных задач, исходя из действующих правовых норм и имеющихся ресурсов и ограничений; УК-2.2 Контролирует ход выполнения проекта, корректирует план-график в соответствии с результатами контроля;
УК-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	УК-3.1 Формулирует и учитывает в своей деятельности особенности поведения групп людей, выделенных в зависимости от поставленной цели; УК-3.2 Анализирует возможные последствия личных действий и планирует свои действия для достижения заданного результата;
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	УК-6.2 Распределяет задачи на долго-, средне- и краткосрочные с обоснованием актуальности и анализа ресурсов для их выполнения;
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1 Обосновывает требования к системе обеспечения информационной безопасности;
ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	ОПК-3.1 Знает порядок разработки и требования к организационно-распорядительным документам по обеспечению информационной безопасности;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Управление информационной безопасностью» 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 «Управление информационной безопасностью».

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-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	Профессиональное общение и межкультурное взаимодействие в команде; Управление проектами;	
УК-2	Способен управлять проектом на всех этапах его жизненного цикла	Управление проектами;	Проектно-технологическая практика; Преддипломная практика;
УК-6	Способен определять и реализовывать приоритеты собственной деятельности и способы ее совершенствования на основе самооценки	Научно-исследовательская работа; Управление проектами;	Информационно-психологическая безопасность; Научно-исследовательская работа; Проектно-технологическая практика; Преддипломная практика;
ОПК-1	Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	Теория игр и исследование операций; Защищенные информационные системы; Технологии обеспечения информационной безопасности;	Информационно-психологическая безопасность; Проектно-технологическая практика;
ОПК-3	Способен разрабатывать проекты организационно-распорядительных документов по обеспечению информационной безопасности	Технологии обеспечения информационной безопасности; Разработка организационно-распорядительных документов по обеспечению информационной безопасности;	Проектно-технологическая практика;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Управление информационной безопасностью» 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)**
			3
Контактная работа, ак.ч.	*68*		*68*
Лекции (**ЛК**)	34		34
Лабораторные работы (**ЛР**)	0		0
Практические/семинарские занятия (**СЗ**)	34		34
Самостоятельная работа обучающихся, ак.ч.	*76*		*76*
Контроль (экзамен/зачет с оценкой), ак.ч.	*36*		*36*
Общая трудоемкость дисциплины	**ак.ч.**	***180***	*180*
	зач.ед.	***5***	*5*

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	Управление ИБ организации как процесс	1.1	Основные понятия, связанные с управлением ИБ Понятия: информационная безопасность, информационная безопасность объекта информатизации, безопасность информации, безопасность информационной технологии и их роль в процессах управления ИБ. Угроза (безопасности информации), уязвимость (объекта защиты), риск ИБ. Сущность управления ИБ организации Необходимость управления обеспечением ИБ организации. Процессный подход к управлению ИБ. Системный подход к управлению ИБ. Управление обеспечением ИБ организации как процесс. Циклическая модель PDCA применительно к управлению ИБ	ЛК, СЗ
Раздел 2	Планирование и организационно-распорядительные документы управления ИБ	2.1	Планирование в управлении ИБ. Определение приоритетов организации для разработки системы управления ИБ организации. Определение области действия системы управления ИБ организации. Определение защищаемых активов информационной инфраструктуры организации, их классификация. Разработка политики системы управления ИБ организации на основе характеристик бизнеса, организации, ее размещения, активов и технологий. Определение подхода к оценке риска в организации. Анализ и оценка рисков. Определение и оценка различных вариантов обработки рисков. Выбор целей и мер управления для обработки рисков	ЛК, СЗ
Раздел 3	Стандарты в области управления ИБ	3.1	Роль стандартов в управлении ИБ. Основные организации, издающие стандарты по вопросам управления ИБ. Международная организация по стандартизации (ИСО, ISO). Международная электротехническая комиссия (МЭК, Национальные органы по стандартизации: Федеральное агентство по техническому регулированию и метрологии (Росстандарт), Британский институт стандартов (BSI), Национальный институт стандартов и технологий США (NIST), Федеральное ведомство по безопасности информационных технологий (BSI, Германия). Общие сведения о стандартах США, Великобритании и Германии, касающихся вопросов управления ИБ. Комплекс стандартов и рекомендаций Банка России по управлению ИБ. Общие требования к системам менеджмента ИБ. Нормы и правила менеджмента ИБ. Цели и меры управления. Организация обеспечения информационной безопасности. Области контроля. Международные стандарты по общим вопросам управления ИБ (ISO 27001, ISO 27002, ISO 27003) и гармонизированные с ними российские национальные стандарты	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
Раздел 4	Внутренние нормативные документы по управлению ИБ организации	4.1	Документационное обеспечение управления информационной безопасностью организации. Задачи и назначение документационного обеспечения управления информационной безопасностью организации. Иерархия внутренних нормативных документов по управлению информационной безопасностью организации. Требования к организации документационного обеспечения управления информационной безопасностью организации. Политика информационной безопасности организации. Роль политики ИБ как основного внутреннего нормативного документа по ИБ. Содержание политики ИБ. Жизненный цикл политики ИБ Другие документы по управлению ИБ. Частные политики ИБ, их назначение и состав. Примеры областей обеспечения ИБ, управляемые частными политиками Документы, содержащие положения ИБ, применяемые к процедурам обеспечения ИБ. Документы, содержащие свидетельства выполненной деятельности по обеспечению ИБ	ЛК, СЗ
Раздел 5	Основные процессы СУИБ. Обязательная документация СУИБ	5.1	Процессы «Управление документами» и «Управление записями» (цели и задачи процессов, входные/выходные данные, роли участников, обязательные этапы процессов, связи с другими процессами СУИБ). Процессы улучшения СУИБ («Внутренний аудит», «Корректирующие действия», «Предупреждающие действия»). Процесс «Мониторинг эффективности» (включая разработку метрик эффективности). Понятие «Зрелость процесса». Процесс «Анализ со стороны высшего руководства». Процесс «Обучение и обеспечение осведомленности».	ЛК, СЗ
Раздел 6	Реализация системы управления ИБ организации	6.1	Планирование в управлении ИБ. Определение приоритетов организации для разработки системы управления ИБ организации. Определение области действия системы управления ИБ организации. Определение защищаемых активов информационной инфраструктуры организации, их классификация. Разработка политики системы управления ИБ организации на основе характеристик бизнеса, организации, ее размещения, активов и технологий. Определение подхода к оценке риска в организации. Анализ и оценка рисков. Определение и оценка различных вариантов обработки рисков. Выбор целей и мер управления для обработки рисков.	ЛК, СЗ
		6.2	Внедрение системы управления информационной безопасностью Разработка плана обработки рисков. Реализация плана обработки рисков для достижения намеченных целей управления. Внедрение мер управления, выбранные на	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
			стадии планирования, для достижения целей управления. Определение способа измерения результативности выбранных мер управления или их групп и использования этих измерений для оценки результативности управления. Реализация программы по обучению и повышению квалификации сотрудников. Управление работой системой управления ИБ организации. Управление ресурсами системы управления ИБ организации. Внедрение процедур и других мер управления, обеспечивающих быстрое обнаружение событий ИБ и реагирование на инциденты, связанные с ИБ	
		6.3	Анализ системы управления ИБ организации. Выполнение процедуры мониторинга, контроля и анализа.	ЛК, СЗ
		6.4	Совершенствование системы управления ИБ организации. Выявление возможностей улучшения системы управления ИБ организации. Выполнение необходимых корректирующих и предупреждающих действий. Передача подробной информации о действиях по улучшению системы управления ИБ организации всем заинтересованным сторонам. Обеспечение внедрения улучшений системы управления ИБ организации для достижения запланированных целей	ЛК, СЗ
Раздел 7	Специальные вопросы управления ИБ организации	7.1	Управление информационной безопасностью финансовых организаций. Требования и рекомендации Банка России и других регуляторов в сфере управления ИБ финансовых организаций. Комплекс СТО БР ИББС. ГОСТ Р 57580.1-2017 «Безопасность финансовых (банковских) операций. Защита информации финансовых организаций. Базовый состав организационных и технических мер» и вопросы его использования. Вопросы ИБ индустрии платежных карт. Отдельные направления менеджмента ИБ. Менеджмент риска информационной безопасности. Менеджмент инцидентов информационной безопасности. Обеспечение непрерывности деятельности и восстановления после прерываний. Обеспечение ИБ на стадиях жизненного цикла автоматизированных систем. Критерии оценки безопасности информационных технологий и автоматизированных систем. Вопросы разработки сценариев по следующим различным ситуациям.	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	Лекционный класс для практической подготовки, проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Комплект специализированной мебели: учебная доска; технические средства: Интерактивная панель 86 дюймов HUAWEI idea Hub S2 IHS2-86SA со встраиваемым OPS компьютером HUAWEI в комплекте с подвижной подставкой HUAWEI idea Hub White Rolling Stand _25, двух объективная PTZ-видеокамера Nearity V520d, Системный блок CPU Intel Core I9-13900F/MSI PRO Z790-S Soc-1700 Intel Z790 / Samsung DDR5 16GB DIMM 5600MHz 2шт/ Samsung SSD 1Tb /Видеокарта RTX3090 2; Монитор LCD LG 27" 27UL500-W белый IPS 3840x2160 5ms 300cd 1000:1 (Mega DCR) DisplayPort P HDMIx2 Audioout, vesa. Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в т. ч. MS Office/Office 365, Teams, Skype). Количество посадочных мест - 28.
Семинарская	Лекционный класс для практической подготовки, проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.	Комплект специализированной мебели: учебная доска; технические средства: Интерактивная панель 86 дюймов HUAWEI idea Hub S2 IHS2-86SA со встраиваемым OPS компьютером HUAWEI в комплекте с подвижной подставкой HUAWEI idea Hub White Rolling Stand _25, двух объективная PTZ-видеокамера Nearity V520d, Системный блок CPU Intel Core I9-13900F/MSI PRO Z790-S Soc-1700 Intel Z790 / Samsung DDR5 16GB DIMM 5600MHz 2шт/ Samsung SSD 1Tb /Видеокарта RTX3090 2; Монитор LCD LG 27" 27UL500-W белый IPS 3840x2160 5ms 300cd 1000:1 (Mega DCR) DisplayPort P HDMIx2 Audioout, vesa. Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в т. ч. MS Office/Office 365, Teams, Skype). Количество посадочных мест - 28.
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.	Компьютерный класс для проведения лабораторно-практических занятий, курсового проектирования, практической подготовки. Комплект специализированной мебели; доска маркерная; технические средства: персональные компьютеры, проекционный экран, мультимедийный проектор, NEC NP-V302XG, выход в Интернет. Программное обеспечение: продукты Microsoft (ОС, пакет офисных приложений, в т.ч. MS Office/Office 365, Teams, Skype), Autodesk AutoCAD 2021, Autodesk AutoCAD 2021 (англ. яз.), Autodesk Inventor 2021, Autodesk Revit 2021, ArchiCAD 23 (бесплатные учебные версии)
		Компьютерный класс - учебная аудитория для практической подготовки, лабораторно-практических занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, а также самостоятельной работы Комплект специализированной мебели; (в т.ч. электронная доска); мультимедийный проектор BenqMP610; экран моторизованный Sharp 228*300; доска аудиторная поворотная; Комплект ПК iRU Corp 317 TWR i7 10700/16GB/ SSD240GB/2TB 7.2K/ GTX1660S-6GB /WIN10PRO64/ BLACK + Комплект Logitech Desktop MK120, (Keybord&mouse), USB, [920-002561] + Монитор HP P27h G4 (7VH95AA#ABB) (УФ-000000000059453)-5шт., Компьютер Pirit Doctrin4шт., ПО для ЭВМ LiraServis Academic Set 2021 Состав пакета ACADEMIC SET: программный комплекс

		"ЛИРА-САПР FULL". программный комплекс "МОНОМАХ-САПР PRO". программный комплекс "ЭСПРИ.

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Воронцова, С. В. Обеспечение информационной безопасности в банковской сфере (Законность и правопорядок) : монография / С. В. Воронцова. — Москва : КноРус, 2021. — 159 с. - ЭБС BOOK.ru. — URL: https://book.ru/book/940132 (дата обращения: 19.04.2024). — Текст : электронный

2.

Дополнительная литература:

1. Курило, А. П. Вопросы управления информационной безопасностью. Основы управления информационной безопасностью : учебное пособие для вузов / А. П. Курило, Н. Г. Милославская, М. Ю. Сенаторов. – Москва : Горячая линия-Телеком, 2013. – 244 с. – ЭБС ZNANIUM. - URL: http://znanium.com/catalog/product/560780 (дата обращения: 19.04.2024). - Текст : электронный

2. Милославская, Н. Г. Вопросы управления информационной безопасностью. Управление рисками информационной безопасности : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - Москва : Горячая линия-Телеком, 2013. - 130 с. - ЭБС ZNANIUM. - URL: http://znanium.com/catalog/product/560781 (дата обращения: 19.04.2024). - Текст : электронный

3. Милославская, Н. Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса : учебное пособие для вузов / Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. - 2-е изд. – Москва : Горячая линия-Телеком, 2016. – 170 с. – ЭБС ZNANIUM. - URL: https://znanium.com/catalog/product/560782 (дата обращения: 19.04.2024). - Текст : электронный

4. Милославская, Н. Г. Технические, организационные и кадровые аспекты управления информационной безопасностью: учебное пособие для вузов/ Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой. – Москва : Горячая линия-Телеком, 2013. – 214 с. – ЭБС ZNANIUM. - URL: http://znanium.com/catalog/product/560783 (дата обращения: 19.04.2024). - Текст : электронный

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 http://lib.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
- ЭБС «Троицкий мост»

2. Базы данных и поисковые системы

- электронный фонд правовой и нормативно-технической документации http://docs.cntd.ru/
- поисковая система Яндекс https://www.yandex.ru/
- поисковая система Google https://www.google.ru/
- реферативная база данных SCOPUS http://www.elsevierscience.ru/products/scopus/

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

1. Курс лекций по дисциплине «Управление информационной безопасностью».

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

8. ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И БАЛЛЬНО-РЕЙТИНГОВАЯ СИСТЕМА ОЦЕНИВАНИЯ УРОВНЯ СФОРМИРОВАННОСТИ КОМПЕТЕНЦИЙ ПО ДИСЦИПЛИНЕ

Оценочные материалы и балльно-рейтинговая система* оценивания уровня сформированности компетенций (части компетенций) по итогам освоения дисциплины «Управление информационной безопасностью» представлены в Приложении к настоящей Рабочей программе дисциплины.

* - ОМ и БРС формируются на основании требований соответствующего локального нормативного акта РУДН.