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

ИНСТРУМЕНТАЛЬНЫЕ СРЕДСТВА АНАЛИЗА РИСКОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

(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 «Инструментальные средства анализа рисков информационной безопасности» 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 5 разделов и 5 тем и направлена на изучение • понятий технологии анализа рисков информационной безопасности; • нормативного обеспечения анализа рисков; • современных методик оценки рисков, принципов построения систем управления рисками информационной безопасности и прикладных средств автоматизации процесса анализа рисков.

Целью освоения дисциплины является - приобретение студентами знаний, умений и навыков в области подготовки о проведения оценки рисков информационной безопасности автоматизированных систем; - освоение дисциплинарных компетенций по применению комплекса мероприятий в системе защиты информации на основе технологии прогнозирования, оценки и обработки рисковинформационной безопасности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Инструментальные средства анализа рисков 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)
ПК-1	Способен оценивать уровень безопасности компьютерных систем и сетей	ПК-1.3 Проводит инструментальный мониторинг защищенности компьютерных систем и сетей;
ПК-3	Способен формировать требования к защите информации в автоматизированных системах	ПК-3.1 Обосновывает необходимость защиты информации в автоматизированной системе; ПК-3.2 Определяет угрозы безопасности информации, обрабатываемой автоматизированной системой; ПК-3.3 Моделирует защищенные автоматизированные системы с целью анализа их уязвимостей и эффективности средств и способов защиты информации;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Инструментальные средства анализа рисков информационной безопасности» относится к части, формируемой участниками образовательных отношений 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 «Инструментальные средства анализа рисков 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*
ПК-1	Способен оценивать уровень безопасности компьютерных систем и сетей	*Системы обнаружения вторжений***; *Методы выявления и анализа инцидентов информационной безопасности***;	Преддипломная практика;
ПК-3	Способен формировать требования к защите информации в автоматизированных системах	*Системы обнаружения вторжений***; *Методы выявления и анализа инцидентов информационной безопасности***;	Преддипломная практика; *Практические аспекты аудита информационной безопасности***; *Обеспечение непрерывности бизнеса***; *Международные аспекты противодействия киберпреступности и кибертерроризму***; *Международно-правовое регулирование в области информационной безопасности***;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Инструментальные средства анализа рисков информационной безопасности» составляет «4» зачетные единицы.

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.	*40*		*40*
Контроль (экзамен/зачет с оценкой), ак.ч.	*36*		*36*
Общая трудоемкость дисциплины	**ак.ч.**	***144***	*144*
	зач.ед.	***4***	*4*

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	Анализ рисков в области информационной безопасности	1.1	Информационная безопасность бизнеса. Проблемы обоснования стоимости корпоративной системы защиты информации. Службы информационной безопасности. Основные функции специалистов, ответственных за информационную безопасность. Основные этапы работы по обеспечению режима информационной безопасности. Постановка задачи анализа рисков. Национальные особенности защиты информации.	ЛК, СЗ
Раздел 2	Стандарты управления рисками	2.1	Национальные стандарты управления рисками информационной безопасности: ГОСТ Р ИСО/МЭК семейств 17799, 27000, 13335, 13569, 18044, 18045. Международные стандарты управления рисками: CobiT, ITIL, BSI, COSO, SAS70, NIST-800. Обзор основных стандартов. Ведомственные и корпоративные стандарты управления рисками информационной безопасности	ЛК, СЗ
Раздел 3	Технологии анализа рисков	3.1	Вопросы анализа рисков и управления ими. Идентификация рисков. Оценивание рисков. Качественные и количественные методики оценки рисков. Выбор допустимого уровня рисков. Выбор контрмер и оценка их эффективности. Разработка корпоративной методики анализа рисков.	ЛК, СЗ
Раздел 4	Средства анализа рисков	4.1	Инструментарии базового уровня. Средства полного анализа рисков. Комплекс оценки рисков «ГРИФ». Методики и инструменты CORAS, CRAMM, Babel Enterprise, RiskWatch. Экспертная система «АванГард».	ЛК, СЗ
Раздел 5	Управление информационными рисками	5.1	Основные элементы управления рисками информационных систем. Система управления информационными рисками	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	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

	контроля и промежуточной аттестации.	/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	Лаборатория для проведения практической подготовки, практико-лабораторных занятий, 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 - 25.
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. Петренко С.А. Управление информационными рисками. Экономически оправданная безопасность / Петренко С.А., Симонов С.В. - М. : Компания АйТи ; ДМК Пресс, 2005.

2. Астахов А.М. Искусство управления информационными рисками -М.: ДМК Пресс, 2010.

3. Зегжда П.Д., Калинин М.О. Управление информационной безопасностью компьютерных систем. - СПб. : Изд-во Политехн. ун-та, 2012.

4. Курило А.П., Милославская Н.Г., Сенаторов М.Ю., Толстой А.И. Управление рисками информационной безопасности. - М. , 2011.

5. Калинин М. О. Теория и системы управления информационной безопасностью. Анализ рисков информационной безопасности : лаб. практикум / М. О. Калинин. - СПб. : Изд-во Политехн. ун-та, 2010

Дополнительная литература:

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации". Принят Государственной Думой 8 июля 2006 года.

2. ГОСТ Р ИСО/МЭК 13335-2007 "Информационная технология. Методы и средства обеспечения безопасности".

3. ГОСТ Р ИСО/МЭК 27001-2006. «Информационные технологии. Методы защиты. Системы менеджмента защиты информации. Требования».

4. ГОСТ Р ИСО/МЭК 18045 «Информационная технология. Методы и средства обеспечения безопасности информационных технологий».

5. ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью».

6. ГОСТ Р ИСО/МэК 13569-2007. «Финансовые услуги. Рекомендации по информационной безопасности».

7. ГОСТ Р ИСО/МЭК 18044-2007 «Информационная технология. Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности».

8. Малюк А.А. Информационная безопасность: концептуальные и методологические основы защиты информации. М.: Горячая Линия - Телеком, 2004.

9. Белов Е.Б., Лось В.П., Мещеряков Р.В., Шелупанов А.А. Основы информационной безопасности: Учебн. пособие для вузов. М: Горячая линия - Телеком, 2006. - 544 с.

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 «Инструментальные средства анализа рисков информационной безопасности».

* - 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 «Инструментальные средства анализа рисков информационной безопасности» представлены в Приложении к настоящей Рабочей программе дисциплины.

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