Федеральное государственное автономное образовательное учреждение высшего образования
«Российский университет дружбы народов имени Патриса Лумумбы»

Факультет физико-математических и естественных наук
(наименование основного учебного подразделения (ОУП)-разработчика ОП ВО)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Кибербезопасность предприятия
(наименование дисциплины/модуля)

Рекомендована МССН для направления подготовки:

38.03.05 Бизнес-информатика
(код и наименование направления подготовки/специальности)

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

Кибербезопасность в экономике
(наименование (профиль/специализация) ОП ВО)

2023 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Кибербезопасность предприятия» является введение учащихся в предметную область современной кибербезопасности предприятия в бизнес-информатике. Для достижения поставленной цели выделяются задачи курса: освоение современных методов обеспечения кибербезопасности предприятия, знакомство слушателей с основами анализа кибербезопасности предприятия и выводами, содержанием категорий, используемых в других дисциплинах, связанных с информационными технологиями.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Кибербезопасность предприятия» направлено на формирование у обучающихся следующих компетенций (части компетенций): УК-2; ПК-3

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-2.1 Знает необходимые для осуществления профессиональной деятельности правовые нормы и методологические основы принятия управленческого решения
		УК-2.2 Умеет определять круг задач в рамках избранных видов профессиональной деятельности, планировать собственную деятельность исходя из имеющихся ресурсов; соотносить главное и второстепенное, решать поставленные задачи в рамках избранных видов профессиональной деятельности
		УК-2.3 Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах
ПК-3	Способен выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	ПК-3.1. Знает основы архитектуры, устройства и функционирования информационно-вычислительных систем и сетевых подсистем инфокоммуникационной системы организации; основы современных операционных систем; сетевые протоколы
		ПК-3.2. Знает основы программирования; современные объектно-ориентированные языки программирования; современные структурные языки программирования; языки современных бизнес-приложений
		ПК-3.3. Умеет кодировать на языках программирования

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Кибербезопасность предприятия» относится к обязательной части блока Б1 ОП ВО.

В рамках ОП ВО обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Кибербезопасность предприятия».

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

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики[1]
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, Правовые основы кибербезопасности, Экономическая безопасность в современных условиях Теневая экономика Киберполитика в международных экономических отношениях	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности) Преддипломная практика
ПК-3	Способность выполнять работы и управлять работами по созданию (модификации) и сопровождению ИС, автоматизирующих задачи организационного управления и бизнес-процессы	Архитектура компьютеров и операционные системы Основы программирования Технология программирования Компьютерный практикум Основы информатики и кибернетики Вычислительные системы, сети и телекоммуникации Основы информационной безопасности	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности) Преддипломная практика

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Кибербезопасность предприятия» составляет 3 зачетных единицы.

Таблица 4.1. Виды учебной работы по периодам освоения ОП ВО

Вид учебной работы		ВСЕГО, ак.ч.	Семестр(-ы)
			7
Контактная работа, ак.ч.		*54*	*54*
в том числе:			
Лекции (**ЛК**)		18	18
Лабораторные работы (**ЛР**)		-	-
Практические/семинарские занятия (**СЗ**)		36	36
Самостоятельная работа обучающихся, ак.ч.		*54*	*54*
Контроль (экзамен/зачет с оценкой), ак.ч.		-	-
Общая трудоемкость дисциплины	ак.ч.	**108**	**108**
	зач.ед.	**3**	**3**

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Наименование раздела дисциплины	Содержание раздела (темы)	Вид учебной работы[2]
Раздел 1. Кибернетики как наука об управлении и организации.	Тема 1.1. Объекты управления. Инструменты управления. Технологии управления.	ЛК, СЗ
	Тема 1.2. Ресурсы управления. Взаимодействие систем.	ЛК, СЗ
	Тема 1.3. Имидж и отношения с окружением.	ЛК, СЗ
Раздел 2. Кибербезопасность предприятия.	Тема 2.1. Активы предприятия. Ущерб предприятия.	ЛК, СЗ
	Тема 2.2. Киберугрозы предприятия. Уязвимости предприятия. Кибератаки на предприятие. Цена кибератаки.	ЛК, СЗ
	Тема 2.3. Возможности противника по организации кибератаки.	ЛК, СЗ
Раздел 3. Контекст деятельности предприятия.	Тема 3.1. Понимание внутренних и внешних факторов деятельности предприятия.	ЛК, СЗ
	Тема 3.2. Понимание потребностей и ожиданий заинтересованных сторон.	ЛК, СЗ
	Тема 3.3. Определение области действия системы менеджмента информационной безопасности.	ЛК, СЗ
Раздел 4. Руководство обеспечением кибербезопасности предприятия.	Тема 4.1. Руководящая роль и обязанности руководства. Политика в области кибербезопасности. Роли, обязанности и полномочия в организации.	ЛК, СЗ
	Тема 4.2. Планирование и действия по обработке рисков и возможностей. Цели информационной безопасности и планы по их достижению.	ЛК, СЗ
	Тема 4.3. Обеспечение и поддержка кибербезопасности. Ресурсы. Квалификация.	ЛК, СЗ

Наименование раздела дисциплины	Содержание раздела (темы)	Вид учебной работы
	Взаимодействие. Документированная информация. Функционирование. Оперативное планирование и контроль кибербезопасности.	
Раздел 5. Меры и средства кибербезопасности предприятия и цели их применения.	Тема 5.1. Внутренняя организация деятельности по обеспечению кибербезопасности. Мобильные устройства и дистанционная работа. Кибербезопасности, связанная с персоналом. Ответственность за активы.	ЛК, СЗ
	Тема 5.2. Физическая безопасность и защита от воздействия окружающей среды. Резервное копирование. Мониторинг кибербезопасности предприятия. Безопасность системы связи.	ЛК, СЗ
	Тема 5.3. Непрерывности бизнеса. Соответствие законам и нормативной базе.	ЛК, СЗ

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.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams. Дополнительное ПО: офисный пакет MS Office или LibreOffice.
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.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams. Дополнительное ПО: офисный пакет MS Office или LibreOffice.

Тип аудитории	Оснащение аудитории	**Специализированное учебное/лабораторное оборудование, ПО и материалы для освоения дисциплины** (при необходимости)
Для самостоятельной работы обучающихся	Аудитория для самостоятельной работы обучающихся (может использоваться для проведения семинарских занятий и консультаций), оснащенная комплектом специализированной мебели и компьютерами с доступом в ЭИОС.	Компьютер/ноутбук с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, MS Teams. Дополнительное ПО: офисный пакет MS Office или LibreOffice.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Внуков А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277
2. Зараменских Е. П. Архитектура предприятия : учебник для вузов / Е. П. Зараменских, Д. В. Кудрявцев, М. Ю. Арзуманян ; под редакцией Е. П. Зараменских. — Москва : Издательство Юрайт, 2022. — 410 с. — (Высшее образование). — ISBN 978-5-534-06712-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493118
3. Нетёсова, О. Ю. Информационные системы и технологии в экономике : учебное пособие для вузов / О. Ю. Нетёсова. — 3-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 178 с. — (Высшее образование). — ISBN 978-5-534-08223-4. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491479

Дополнительная литература:

1. Внуков, А. А. Защита информации в банковских системах : учебное пособие для вузов / А. А. Внуков. — 2-е изд., испр. и доп. — Москва : Издательство Юрайт, 2022. — 246 с. — (Высшее образование). — ISBN 978-5-534-01679-6. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490278
2. Грекул, В. И. Проектирование информационных систем : учебник и практикум для вузов / В. И. Грекул, Н. Л. Коровкина, Г. А. Левочкина. — Москва : Издательство Юрайт, 2022. — 385 с. — (Высшее образование). — ISBN 978-5-9916-

8764-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489918
3. Казарин О. В. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов / О. В. Казарин, А. С. Забабурин. — Москва : Издательство Юрайт, 2022. — 312 с. — (Высшее образование). — ISBN 978-5-9916-9043-0. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/491249
4. Казарин, О. В. Основы информационной безопасности: надежность и безопасность программного обеспечения : учебное пособие для среднего профессионального образования / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Профессиональное образование). — ISBN 978-5-534-10671-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/495524
5. Полякова Т. А. Организационное и правовое обеспечение информационной безопасности : учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственные редакторы Т. А. Полякова, А. А. Стрельцов. — Москва : Издательство Юрайт, 2022. — 325 с. — (Профессиональное образование). — ISBN 978-5-534-00843-2. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/498889
6. Щербак А. В. Информационная безопасность : учебник для среднего профессионального образования / А. В. Щербак. — Москва : Издательство Юрайт, 2022. — 259 с. — (Профессиональное образование). — ISBN 978-5-534-15345-3. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/497642

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 «Лань» http://e.lanbook.com/
- 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[3]:

1. Курс лекций по дисциплине «Кибербезопасность предприятия».
2. Практические задания по дисциплине «Кибербезопасность предприятия».

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

Оценочные материалы и балльно-рейтинговая система[4] оценивания уровня сформированности компетенций (части компетенций) по итогам освоения дисциплины «Кибербезопасность предприятия» представлены в Приложении к настоящей Рабочей программе дисциплины.

РАЗРАБОТЧИКИ:

Профессор кафедры прикладной информатики и теории вероятностей		А.А. Грушо
Должность, БУП	Подпись	Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Зав. кафедрой прикладной информатики и теории вероятностей		К.Е. Самуйлов
Наименование БУП	Подпись	Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Зав. кафедрой прикладной информатики и теории вероятностей		К.Е. Самуйлов
Должность, БУП	Подпись	Фамилия И.О.

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

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