

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ястребов Олег Александрович
Должность: Ректор
Дата подписания: 05.09.2023 15:22:09
Уникальный программный ключ:
ca953a0120d891083f939673078ef1a989dae18a

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

Высшая школа промышленной политики и предпринимательства

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Обеспечение кибербезопасности хозяйствующего субъекта

(наименование дисциплины/модуля)

Рекомендована МСЧН для направления подготовки/специальности:

38.04.01 «ЭКОНОМИКА»

(код и наименование направления подготовки/специальности)

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

«Комплаенс-контроль в деятельности организаций»

(наименование (профиль/специализация) ОП ВО)

2023 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ:

Цель изучения дисциплины «Обеспечение кибербезопасности хозяйствующего субъекта» - формирование системного представления о зарубежном опыте организации и управления внутренним контролем и аудитом в системе экономической безопасности, а также на развитие практических навыков в области организации и управления комплаенс-контролем.

Основными задачами изучения дисциплины являются:

исследование основных понятий в области безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры(КИИ);

основных угроз, уязвимостей, рисков в области безопасности Интернета вещей, киберфизических систем в составе объектов критической информационной инфраструктуры;

технологий угроз сетевой безопасности, а также механизмов противодействия сетевым атакам;

основных требований нормативно-правовых документов по защите объектов критической информационной инфраструктуры; •особенностей проектирования

2.ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ:

Освоение дисциплины «Обеспечение кибербезопасности хозяйствующего субъекта» 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-1	Способен осуществлять поиск, критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий	УК-1.1. Анализирует задачу, выделяя ее базовые составляющие; УК-1.2. Определяет и ранжирует информацию, требуемую для решения поставленной задачи; УК-1.3. Осуществляет поиск информации для решения поставленной задачи по различным типам запросов; УК-1.4. Предлагает варианты решения задачи, анализирует возможные последствия их использования; УК-1.5. Анализирует пути решения проблем мировоззренческого, нравственного и личностного характера на основе использования основных философских идей и категорий в их историческом

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
		развитии и социально-культурном контексте.
УК-3	Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели	<p>УК-3.1. Определяет свою роль в команде, исходя из стратегии сотрудничества для достижения поставленной цели;</p> <p>УК-3.2. Формулирует и учитывает в своей деятельности особенности поведения групп людей, выделенных в зависимости от поставленной цели;</p> <p>УК-3.3. Анализирует возможные последствия личных действий и планирует свои действия для достижения заданного результата;</p> <p>УК-3.4. Осуществляет обмен информацией, знаниями и опытом с членами команды;</p> <p>УК-3.5. Аргументирует свою точку зрения относительно использования идей других членов команды для достижения поставленной цели;</p> <p>УК-3.6. Участвует в командной работе по выполнению поручений.</p>
ПК-4	Способен разработать и сформировать отчетные документы о работе системы внутреннего контроля экономического субъекта	ПК-4.1 Способен оценивать возможные последствия изменений в учетной политике экономического субъекта, в том числе их влияние на его дальнейшую деятельность
ПК-5	Способен осуществлять контроль и координацию деятельности систем внутреннего контроля на всех уровнях управления экономическим субъектом	ПК-5.1 Способен анализировать и толковать нормы и требования нормативных правовых актов по внутреннему контролю деятельности организации, регламентирующие вопросы независимости и принципы этики

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО:

Дисциплина «Обеспечение кибербезопасности хозяйствующего субъекта» относится к элективной части, формируемой участниками образовательных отношений.

В таблице № 1 приведены предшествующие и последующие дисциплины, направленные на формирование компетенций дисциплины в соответствии с матрицей компетенций ОП ВО.

В рамках ОП ВО обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Обеспечение кибербезопасности хозяйствующего субъекта».

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-1	Способен осуществлять поиск, критический анализ проблемных ситуаций на основе системного подхода, выработать стратегию действий	Микроэкономика (продвинутый курс), Макроэкономика (продвинутый курс), Внутренний контроль, Международные и российские стандарты в области внутреннего контроля и аудита, Методы комплексного анализа деятельности хозяйствующего субъекта, Управление эффективностью комплаенс-контроля хозяйствующего субъекта, Риск-менеджмент и комплаенс	
УК-3	Способен организовывать и руководить работой команды, выработывая командную стратегию для достижения поставленной цели	Микроэкономика (продвинутый курс), Макроэкономика (продвинутый курс), Эконометрика (продвинутый курс), Внутренний контроль, Методы комплексного анализа деятельности хозяйствующего субъекта, Международные и российские стандарты в области внутреннего контроля и аудита, Методы комплексного анализа деятельности хозяйствующего субъекта, Управление эффективностью комплаенс-контроля хозяйствующего субъекта, Риск-менеджмент и комплаенс, Оценка коррупционных рисков хозяйствующего субъекта,	

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
		Налоговый комплаенс	
ПК-4	Способен разработать и сформировать отчетные документы о работе системы внутреннего контроля экономического субъекта	Микроэкономика (продвинутый курс), Макроэкономика (продвинутый курс), Внутренний контроль, Методы комплексного анализа деятельности хозяйствующего субъекта, Цифровые технологии в системе контроля, Система комплаенс-контроля при проведении финансовых расследований, Риск-менеджмент и комплаенс, Противодействие корпоративному мошенничеству, Налоговый комплаенс	
ПК-5	Способен осуществлять контроль и координацию деятельности систем внутреннего контроля на всех уровнях управления экономическим субъектом	Микроэкономика (продвинутый курс), Макроэкономика (продвинутый курс), Внутренний контроль, Цифровые технологии в системе контроля, Управление эффективностью комплаенс-контроля хозяйствующего субъекта, Риск-менеджмент и комплаенс, Противодействие корпоративному мошенничеству, Налоговый комплаенс	

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Обеспечение кибербезопасности хозяйствующего субъекта» составляет 3 зачетных единиц.

Таблица 4.1. Виды учебной работы по периодам освоения ОП ВО для **ОЧНОЙ** формы обучения

Вид учебной работы	ВСЕГО, ак.ч.	Семестр(-ы)			
		1	2	3	4
<i>Контактная работа, ак.ч.</i>	36			54	
в том числе:					
Лекции (ЛК)	18			18	
Лабораторные работы (ЛР)					
Практические/семинарские занятия (СЗ)	36			36	
<i>Самостоятельная работа обучающихся, ак.ч.</i>	54			45	
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	18			9	
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*
Раздел 1. Кибербезопасность: основные понятия и определения	Кибербезопасность (информационная безопасность) киберфизических систем, кибербезопасность в «Интернет-вещей»: основные стандарты, понятия, определения. Киберфизические системы и «Интернет-вещей»: обзор основных проблем, связанных с кибербезопасностью; основные угрозы и уязвимости в сфере кибербезопасности.	ЛК, СЗ
Раздел 2. Сетевые технологии и протоколы: основные понятия и определения	Сетевые технологии и протоколы – модель OSI, проблемы безопасности.	ЛК, СЗ
Раздел 3. Функциональная безопасность: основные понятия и определения	Функциональная безопасность: основные стандарты, понятия и определения.	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)	21 рабочее место: сист.блок P4 C2D/3160 MHz MB/ 320

Тип аудитории	Оснащение аудитории	Специализированное учебное/лабораторное оборудование, ПО и материалы для освоения дисциплины (при необходимости)
	и техническими средствами мультимедиа презентаций.	GB/DVD±RW/ LCD monitor 19"+ 1 проектор
Лаборатория	Аудитория для проведения лабораторных работ, индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная комплектом специализированной мебели и оборудованием.	21 рабочее место: сист.блок Celeron /2600 MHz/1280 MB/ 40 GB/DVD ROM/ LCD monitor 17"+ 1 проектор + Точка доступа WiFi
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.	21 рабочее место: сист.блок P4 C2D/3160 MHz MB/ 320 GB/DVD±RW/ LCD monitor 19"+ 1 проектор
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оснащенная персональными компьютерами (в количестве ___ шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	21 рабочее место: сист.блок Celeron /2600 MHz/1280 MB/ 40 GB/DVD ROM/ LCD monitor 17"+ 1 проектор + Точка доступа WiFi
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.	420 ауд.

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Международная информационная безопасность: Теория и практика: В трех томах. Том 2: Сборник документов (на русском языке) / Под общ. ред. А. В. Крутских. — М.: Издательство «Аспект Пресс», 2023. — 784 с.
2. Суворова, Г. М. Информационная безопасность: учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3. — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: <https://urait.ru/bcode/531084>

Дополнительная литература:

Вострецова, Е.В. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В.Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с.

электронные источники:

- www.minfin.ru – сайт Министерства Финансов РФ.
- www.cbr.ru – сайт Банка России
- www.interfax.ru – сайт Интерфакс
- www.kommersant.ru – сайт Коммерсантъ
- www.rbc.ru – сайт РосБизнесКонсалтинг
- www.vedomosti.ru – сайт Ведомости
- www.Int-comp.org/careers/a-career-in-compliance/ – сайт Международной ассоциации комплаенса

Ресурсы информационно-телекоммуникационной сети «Интернет»:

а) программное обеспечение

Microsoft Office, Mentor

б) базы данных, информационно-справочные и поисковые системы

1. Сайт библиотеки РУДН – Режим доступа: <http://lib.rudn.ru/> - со стационарных компьютеров РУДН
2. Университетская библиотека ONLINE – Режим доступа: <http://www.biblioclub.ru/>
3. LexisNexis. – Режим доступа: <http://www.lexisnexis.com/hottopics/lnacademic/>
4. Книжные коллекции издательства SPRINGER. – Режим доступа: www.springerlink.com
5. Вестник РУДН – Режим доступа: <http://www.elibrary.ru/defaultx.asp>
6. Columbia International Affairs Online (CIAO) – Режим доступа: <http://www.ciaonet.org/>
7. Универсальные базы данных East View. – Режим доступа: <http://online.ebiblioteka.ru/>
8. Полнотекстовая коллекция российских научных журналов. eLibrary.ru – Режим доступа: <http://elibrary.ru/defaultx.asp?>
9. Электронная библиотека Издательского дома «Гребенников». Grebennikon. – Режим доступа: <http://grebennikon.ru/>
10. Международный портал электронных газет общественно-политической тематики. Library PressDisplay – Режим доступа: <http://library.pressdisplay.com>
11. Справочники - отраслевые и страноведческие БД. Polpred.com. – Режим доступа: <http://www.polpred.com/>
12. On-line доступ к журналам. Информационная база данных по всем отраслям науки и электронная доставка документов. SwetsWise. – Режим доступа: <https://www.swetswise.com>
13. Журналы University of Chicago Press Journals: American Journal of Education. Comparative Education Review. – Режим доступа: <http://www.journals.uchicago.edu/action/showJournals?type=byAlphabet>
14. Книги издательства «Альпина Паблишерз». Актуальная деловая литература. – Режим доступа: http://www.alpinabook.ru/books/online_biblioteka.php
15. Электронная библиотека литературы по истории России BIBLIOPHIKA – Режим доступа: <http://www.bibliophika.ru/>
16. Электронная библиотека диссертаций РГБ – Режим доступа: <http://diss.rsl.ru/>
Поисковые системы : Яндекс (yandex.ru), Google (google.ru)

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

1. Курс лекций по дисциплине «Обеспечение кибербезопасности хозяйствующего субъекта».

2. 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

Практические занятия по дисциплине «Обеспечение кибербезопасности хозяйствующего субъекта» служат для закрепления и усвоения теоретического материала лекций и самостоятельной работы студентов с учебной литературой, а также для текущего контроля знаний студентов по дисциплине. На практические занятия вынесены темы и задачи, требующие глубокого теоретического освоения материала и его практического применения. Групповое обсуждение этих тем студентами совместно с преподавателем должно привести к пониманию системных взаимосвязей между анализируемыми процессами и явлениями в стратегическом управлении. Закрепление теоретического материала осуществляется путем экономико-математического моделирования ситуационных задач по микроэкономике.

Основными формами проведения практических занятий по дисциплине «Зарубежная практика применения комплаенс-контроля в деятельности хозяйствующего субъекта» следует считать:

- устный опрос;
- научная дискуссия;
- доклад;
- письменное решение задач;
- письменное решение тестов;
- самостоятельная работа (летучка);
- письменная контрольная работа (в течение учебной пары).

В силу ограниченного времени на проведение семинарских занятий целесообразно в ходе семинара сочетать разные формы обучения и контроля.

Реализация курса предусматривает интерактивные лекции, практические занятия (семинары) с использованием мультимедийного оборудования, подготовку самостоятельных творческих работ и их последующие презентации, тестирование, проведение групповых дискуссий по тематике курса, современные технологии контроля знаний.

Изучая дисциплину, студент должен прослушать курс лекций, пройти предусмотренное рабочей программой количество семинарских занятий, самостоятельно изучить некоторые темы курса и подтвердить свои знания в ходе контрольных мероприятий.

Работа студента на лекции заключается в уяснении основ дисциплины, кратком конспектировании материала, уточнении вопросов, вызывающих затруднения. Конспект лекций является базовым учебным материалом наряду с учебниками, рекомендованными в основном списке литературы.

Преподавание основной части лекционного материала происходит с использованием средств мультимедиа, которые облегчают восприятие и запоминание материала. Презентации доступны для скачивания с сайта РУДН и могут свободно использоваться студентами в учебных целях.

Студент обязан освоить все темы, предусмотренные учебно-тематическим планом дисциплины. Отдельные темы и вопросы обучения выносятся на самостоятельное изучение. Студент изучает рекомендованную литературу и кратко конспектирует материал, а наиболее сложные вопросы, требующие разъяснения, уточняет во время консультаций. Аналогично следует поступать с разделами курса, которые были пропущены в силу различных обстоятельств.

Для углублённого изучения вопроса студент должен ознакомиться с литературой

из дополнительного списка и специализированными сайтами в Интернет. Рекомендуется так же общение студентов на форумах профессиональных сообществ.

Студенты самостоятельно изучают учебную, научную и периодическую литературу. Они имеют возможность обсудить прочитанное с преподавателями дисциплины во время плановых консультаций, с другими студентами на семинарах, а также на лекциях, задавая уточняющие вопросы лектору.

Контроль самостоятельной работы магистров осуществляет ведущий преподаватель. В зависимости от методики преподавания могут быть использованы следующие формы текущего контроля: краткий устный или письменный опрос перед началом занятий, письменное домашнее задание, рефераты и пр.

Примерная структура типового практического занятия:

1. Массовая проверка знания определений и формул по пройденному материалу (последние 1-2 лекции) с помощью письменной летучки в течение 5-10 мин. на отдельных листах.

(обеспечивает 100% охват студентов в группе; стимулирует планомерное освоение формул и определений)

2. Проверка письменного домашнего задания (задач и тестов) с разбором у доски заданий, вызвавших наибольшее затруднение в течение 5-10 мин. в зависимости от сложности. Выставление оценок.

(обеспечивает заинтересованность студентов в выполнении письменных домашних заданий и получении практических навыков решения задач по микроэкономике)

3. Устный опрос по текущему материалу или 1 доклад в течение 10-20 мин.

(с целью обсуждения наиболее сложных теоретических вопросов и развития навыков устной речи)

4. Объяснение методики решения задач и тестов по новой теме преподавателем в течение 5-10 мин.

(обеспечивает новый взгляд студентов на теоретические модели микроэкономики, закрепляет практические навыки)

1. Самостоятельное решение задач и тестов по новой теме в течение оставшегося времени с разбором решения у доски.

(100% охват студентов группы; освоение теоретического материала в ходе решения практических заданий; развитие навыков практического экономического анализа; элемент соревнования - кто решит быстрее)

2. Подведение итогов семинарского занятия: выставление оценок и выдача домашнего задания в течение 2-3 мин.

Аттестация студентов по курсу «Обеспечение кибербезопасности хозяйствующего субъекта» проводится по балльно-рейтинговой системе:

Максимальное количество баллов – 100.

Количество кредитов – 4.

Максимальное количество баллов за выполнение каждого вида работ:

1. опрос – 20 баллов
2. выполнение ДЗ – 20 баллов
3. работа на занятии – 20 баллов
4. доклад – 10 баллов
5. промежуточная КР – 10 баллов
6. итоговая КР – 20 баллов;

Оценка **неудовлетворительно** выставляется в форме F(2); FX(2+).

Оценка F(2) выставляется при условии, если студент набрал менее 30 баллов, оценка FX(2+) – 31-50 баллов. Оценка FX(2+) даёт возможность для пересдачи экзамена или зачёта.

Оценка *удовлетворительно* выставляется в форме E(3); D(3+). Оценка E(3) выставляется при условии, если студент набрал от 51 до 60 баллов. Оценка D(3+) – при условии наличия 61-68 баллов.

Оценка *хорошо* выставляется в форме C(4) при условии, если студент набрал 69-85 баллов.

Оценка *отлично* выставляется в форме B(5); A(5+). Оценка B(5) выставляется, если студент набрал 86-94 балла и свидетельствует о выполнении всех требуемых условий прохождения курса. Оценка A(5+) – 95-100 баллов выставляется не только при условии выполнения всех требований, но и с обязательным проявлением творческого отношения к предмету, умения находить оригинальные, не содержащиеся в учебниках ответы, умения работать с источниками, которые содержатся в дополнительной литературе к курсу, умения соединять знания, полученные в данном курсе со знаниями других дисциплин.

Баллы БРС	Традиционные оценки РФ	Оценки ECTS
95 – 100	Отлично – 5	A (5+)
86 – 94		B (5)
69 – 85	Хорошо – 4	C (4)
61 – 68	Удовлетворительно – 3	D (3+)
51 – 60		E (3)
31 – 50	Неудовлетворительно – 2	FX (2+)
0 – 30		F (2)
51 - 100	Зачет	Passed

РАЗРАБОТЧИКИ:

Заведующий кафедрой
«Комплаенс и контроллинг»



Рагулина Ю.В.

Должность, БУП

Подпись

Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой
«Комплаенс и контроллинг»



Рагулина Ю.В.

Наименование БУП

Подпись

Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой
«Комплаенс и контроллинг»



Рагулина Ю.В.

Должность, БУП

Подпись

Фамилия И.О.