

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ястребов Олег Александрович
Должность: Ректор
Дата подписания: 26.05.2023 17:29:17
Уникальный программный ключ:
ca953a0120d891083f939673078ef1a989dae18a

**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

Анализ и показатели эффективности кибербезопасности 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 «Анализ и показатели эффективности кибербезопасности предприятия» является изучение принципов анализа эффективности кибербезопасности предприятия, знакомство с нормативной базой, подходами к анализу инцидентов кибербезопасности и принципами безопасного использования криптографических средств.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Анализ и показатели эффективности кибербезопасности предприятия» направлено на формирование у обучающихся следующих компетенций (части компетенций): ПК-1, ПК-5

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 проводить работы по обработке и анализу научно-технической информации и результатов исследований	ПК-1.1. Знает методы анализа и обобщения отечественного и международного опыта в соответствующей области исследования
		ПК-1.2. Умеет применять методы анализа научно-технической информации для решения стандартных задач в собственной профессиональной и научно-исследовательской деятельности
		ПК-1.3. Владеет базовыми навыками подготовки научных обзоров и (или) публикаций, рефератов и библиографий по тематике проводимых исследований на русском и иностранном языке
ПК-5	Способен решать задачи управления кибербезопасностью предприятий и иных экономических систем	ПК-5.1. Знает методы организации управления кибербезопасностью предприятий и иных экономических систем
		ПК-5.2. Знает основы нормативно-правового регулирования в РФ и иных странах в области защиты информации
		ПК-5.3. Умеет применять методы управления кибербезопасностью предприятий и иных экономических систем
		ПК-5.4. Умеет использовать нормативно-правовую базу РФ и иных стран в области защиты информации в процессе управления кибербезопасностью предприятий и иных экономических систем
		ПК-5.5. Владеет навыками организации управления кибербезопасностью предприятий и иных экономических систем

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
		ПК-5.6. Владеет навыками применения нормативно-правовой базы РФ и иных стран в области защиты информации в процессе управления кибербезопасностью предприятий и иных экономических систем

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Анализ и показатели эффективности кибербезопасности предприятия» относится к части, формируемой участниками образовательных отношений, блока Б1 ОП ВО.

В рамках ОП ВО обучающиеся также осваивают другие дисциплины и/или практики, способствующие достижению запланированных результатов освоения дисциплины «Анализ и показатели эффективности кибербезопасности 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
ПК-1	Способен проводить работы по обработке и анализу научно-технической информации и результатов исследований	Источники угроз кибербезопасности	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы), Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности), Преддипломная практика
ПК-5	Способен решать задачи управления кибербезопасностью предприятий и иных экономических систем	Цифровая трансформация глобальной экономики, Экономическая безопасность в современных условиях, Источники угроз кибербезопасности, Технологии обеспечения кибербезопасности	Искусственный интеллект и кибербезопасность, Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности), Преддипломная практика

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

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики
		предприятий, Противодействие несанкционированным воздействиям в киберпространстве	

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Анализ и показатели эффективности кибербезопасности предприятия» составляет 4 зачетные единицы.

Таблица 4.1. Виды учебной работы по периодам освоения ОП ВО

Вид учебной работы	ВСЕГО, ак.ч.	Семестр(-ы)
		6
Контактная работа, ак.ч.	72	72
Лекции (ЛК)	36	36
Лабораторные работы (ЛР)	-	-
Практические/семинарские занятия (СЗ)	36	36
Самостоятельная работа обучающихся, ак.ч.	45	45
Контроль (экзамен/зачет с оценкой), ак.ч.	27	27
Общая трудоемкость дисциплины	ак.ч.	144
	зач.ед.	4

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. Основные принципы и подходы к установлению доверия к кибербезопасности предприятия	Тема 1.1. Обеспечение доверия за счет выполнения критериев кибербезопасности.	ЛК, СЗ
	Тема 1.2. Основные принципы и подходы к установлению доверия к кибербезопасности в стандарте ИСО15498. Шкала оценки доверия в ИСО 15408. Требования доверия к кибербезопасности.	ЛК, СЗ
	Тема 1.3. Доверие на основе учета уязвимостей. Доверие через оценку. Структура классов доверия. Уровни доверия. Угрозы и политики.	ЛК, СЗ

2 - заполняется только по ОЧНОЙ форме обучения: ЛК – лекции; ЛР – лабораторные работы; СЗ – семинарские занятия.

Наименование раздела дисциплины	Содержание раздела (темы)	Вид учебной работы
Раздел 2. Нормативная база по обеспечению кибербезопасности.	Тема 2.1. Обеспечение доверия через выполнение требований регуляторов.	ЛК, СЗ
	Тема 2.2. Системы сертификации и аттестации.	ЛК, СЗ
	Тема 2.3. Организация сертификации по требованиям ФСТЭК, ФСБ и ИСО 15408. Задание по кибербезопасности.	ЛК, СЗ
Раздел 3. Анализ аномалий и инцидентов кибербезопасности.	Тема 3.1. Классификация аномалий и инцидентов кибербезопасности.	ЛК, СЗ
	Тема 3.2. Поиск аномалий и признаков инцидентов кибербезопасности.	ЛК, СЗ
	Тема 3.3. SIEM системы.	ЛК, СЗ
Раздел 4. Безопасное использование криптографии	Тема 4.1. Электронный документооборот.	ЛК, СЗ
	Тема 4.2. Необходимость использования сертификатов открытых ключей.	ЛК, СЗ
	Тема 4.3. Генерация ключей. Криптографическая аутентификация.	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.	-
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 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, GNU Octave, Scilab

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Модели безопасности компьютерных систем : учебное пособие / П.Н. Девянин. - М. : Академия, 2005. - 144 с. - (Высшее профессиональное образование). - ISBN 5-7695-2053-1 : 0.00.
2. 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].

Дополнительная литература:

1. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 209 с. — (Высшее образование). — ISBN 978-5-9916-7088-3. — Текст : электронный // Образовательная платформа Юрайт [сайт].
2. Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для вузов / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2022. — 245 с. — (Высшее образование). — ISBN 978-5-9916-7090-6. — Текст : электронный // Образовательная платформа Юрайт [сайт].
3. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5.
4. Информационные системы в экономике и защита информации на предприятиях - участниках ВЭД : учебное пособие / А.В. Астахова. - Электронные текстовые данные. - Санкт-Петербург : Троицкий мост, 2014. - 214 с. : ил. - ISBN 978-5-4377-0040-2.

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/модуля³:

1. Курс лекций по дисциплине «Анализ и показатели эффективности кибербезопасности предприятия».
2. Сборник задач по дисциплине «Анализ и показатели эффективности кибербезопасности предприятия»

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 «Анализ и показатели эффективности кибербезопасности предприятия» представлены в Приложении к настоящей Рабочей программе дисциплины.

РАЗРАБОТЧИКИ:

Доцент кафедры прикладной информатики и теории вероятностей

Должность, БУП



Подпись

С.Ю. Мельников

Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Зав. кафедрой прикладной информатики и теории вероятностей

Наименование БУП



Подпись

К.Е. Самуйлов

Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Зав. кафедрой прикладной информатики и теории вероятностей

Должность, БУП



Подпись

К.Е. Самуйлов

Фамилия И.О.

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