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/специальности:

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)

2026 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Анализ и показатели эффективности кибербезопасности предприятия» входит в программу бакалавриата «Кибербезопасность в экономике» по направлению 38.03.05 «Бизнес-информатика» и изучается в 6 семестре 3 курса. Дисциплину реализует Кафедра теории вероятностей и кибербезопасности. Дисциплина состоит из 4 разделов и 12 тем и направлена на изучение принципов анализа эффективности кибербезопасности предприятия.

Целью освоения дисциплины является формирование у обучающихся системных компетенций в области принципов оценки и анализа эффективности кибербезопасности предприятия, знакомство с нормативной базой, подходами к анализу инцидентов кибербезопасности и принципами безопасного использования криптографических средств, а также развитие практических компетенций по анализу и оценке защищенности информационных систем.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Анализ и показатели эффективности кибербезопасности предприятия» 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 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	Владеет навыками организации 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 навыкками организации управления кибербезопасностью предприятий и иных экономических систем; 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 блоку по выбору блока образовательной программы высшего образования.

В рамках образовательной программы высшего образования 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***
ПК-1	Способен проводить работы по обработке и анализу научно-технической информации и результатов исследований	Источники угроз кибербезопасности;	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика; Seminar-Discussion on Business Informatics;
ПК-5	Владеет навыками организации управления кибербезопасностью предприятий и иных экономических систем	Экономическая безопасность; Источники угроз кибербезопасности; Технологии обеспечения кибербезопасности предприятий; Противодействие несанкционированным воздействиям в киберпространстве; Экономическая оценка угроз кибербезопасности; Бизнес-аналитика и методы принятия решений; Экономика "Умного города" и обеспечение безопасности ее функционирования;	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика; Искусственный интеллект и кибербезопасность; Технологии распределенного реестра Blockchain; Финансовая безопасность; Практикум по кибербезопасности предприятия. Часть 2;

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

** - элективные дисциплины /практики

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 образовательной программы высшего образования для очной формы обучения.

Вид учебной работы	**ВСЕГО,** ак.ч.		**Семестр(-ы)**
			6
Контактная работа, ак.ч.	*72*		*72*
Лекции (**ЛК**)	36		36
Лабораторные работы (**ЛР**)	0		0
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***	*144*
	зач.ед.	***4***	*4*

5. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

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

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
Раздел 1	Основные принципы и подходы к установлению доверия к кибербезопасности предприятия	1.1	Обеспечение доверия за счет выполнения критериев кибербезопасности	Понятие доверия как функции соблюдения заданных критериев. Классификация критериев кибербезопасности (технические, организационные, процессуальные). Критерии как измеримые индикаторы защищённости. Верификация выполнения критериев (аудит, тестирование, контроль). Корреляция между полнотой выполнения критериев и уровнем доверия. Количественные и качественные шкалы оценки соблюдения критериев. Практическое значение: применение критериев при аттестации и сертификации.	ЛК, СЗ
		1.2	Основные принципы и подходы к установлению доверия к кибербезопасности в стандарте ИСО15498. Шкала оценки доверия в ИСО 15408. Требования доверия к кибербезопасности	Общая характеристика стандарта ISO/IEC 15408 («Общие критерии»). Принципы установления доверия в ISO 15408: независимая оценка, воспроизводимость. Шкала уровней EAL. Функциональные требования безопасности (SFR). Требования доверия к безопасности (SAR). Взаимосвязь EAL, SFR и SAR в процедуре сертификации. Практическое применение стандарта для оценки продуктов и систем.	ЛК, СЗ
		1.3	Доверие на основе учета уязвимостей. Доверие через оценку. Структура классов доверия. Уровни доверия. Угрозы и политики.	Понятие доверия через анализ уязвимостей (обратная зависимость). Доверие через оценку: тестирование на проникновение, аудит безопасности. Классы доверия: назначение и структура. Уровни доверия: градации надёжности системы в различных условиях. Модель угроз как исходная предпосылка для установления доверия. Политики безопасности как управляющая основа доверия. Взаимосвязи угроз, уязвимостей, политик, уровня доверия. Практическое значение для управления кибербезопасностью предприятия.	ЛК, СЗ
Раздел 2	Нормативная база по обеспечению кибербезопасности	2.1	Обеспечение доверия через выполнение требований регуляторов.	Понятие регулятора в сфере кибербезопасности (государственные органы, отраслевые надзорные органы). Основные виды регуляторных требований (законы, приказы, стандарты). Доверие как следствие подтвержденного соответствия этим требованиям. Формы контроля выполнения требований (проверки, отчётность, аудит). Ответственность за невыполнение регуляторных требований (административная, уголовная). Практическое значение: снижение рисков и	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				повышение доверия со стороны государства и контрагентов.	
		2.2	Системы сертификации и аттестации.	Определение сертификации (подтверждение соответствия требованиям безопасности). Определение аттестации (оценка состояния защищённости конкретного объекта информатизации). Различие между сертификацией (продукт/система в целом) и аттестацией (конкретный экземпляр в конкретных условиях). Национальные и международные системы сертификации. Этапы сертификации и аттестации. Роль аккредитованных испытательных лабораторий. Сертификат соответствия и аттестат соответствия: структура и срок действия. Практическое значение: доверие как легитимное подтверждение безопасности для заказчиков и рынка.	ЛК, СЗ
		2.3	ГОСТ Р ИСО/МЭК 27004—2021. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание.	Общая характеристика стандарта как адаптации международного ISO/IEC 27004. Место стандарта в семействе ГОСТ Р ИСО/МЭК 27000. Мониторинг, измерение, анализ и оценивание СМИБ (системы менеджмента информационной безопасности). Различие между мониторингом (непрерывное наблюдение) и оцениванием (периодическая оценка). Метрики и показатели результативности СМИБ. Оценка защищённости как объективная мера эффективности средств защиты. Анализ и оценивание: обработка результатов мониторинга для принятия решений. Практическое применение стандарта для постоянного улучшения и демонстрации доверия.	ЛК, СЗ
Раздел 3	Меры обеспечения кибербезопасности предприятия	3.1	Классификация мер обеспечения кибербезопасности.	Понятие меры обеспечения кибербезопасности. Цель классификации: системный подход к выбору и обоснованию мер. Классификация по природе мер (организационные, технические, криптографические, физические). Классификация по этапу жизненного цикла (превентивные, обнаруживающие, реагирующие, восстанавливающие). Классификация по уровню управления (стратегические, тактические, операционные). Классификация по объекту защиты (защита персонала, процессов, данных, инфраструктуры). Классификация по способу реализации (административные, программно-аппаратные, правовые). Практическое значение: выбор адекватных мер в зависимости от угроз и ресурсов	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				предприятия.	
		3.2	Организационные меры обеспечения кибербезопасности. Физическая безопасность.	Понятие организационных мер (управленческие, режимные, административные). Разработка и внедрение политик, регламентов, процедур и инструкций. Назначение ответственных лиц и разграничение зон ответственности. Планирование резервного копирования и восстановления. Управление инцидентами: обнаружение, анализ, реагирование. Контроль доступа на территорию и в помещения (пропускной режим, видеонаблюдение). Защита серверных, коммутационных и хранилищ данных. Практическое значение: предотвращение утечек и разрушений через физический доступ.	ЛК, СЗ
		3.3	Работа с персоналом предприятия. Особенности служебной документации и должностных инструкций сотрудников.	Персонал как ключевой элемент кибербезопасности и основная уязвимость. Подбор и приём на работу: проверка благонадёжности, подписание соглашений о неразглашении. Внедрение документированных регламентов работы с конфиденциальной информацией. Должностные инструкции: явное закрепление обязанностей по соблюдению мер кибербезопасности. Регулярное обучение, повышение осведомлённости и проверка знаний. Процедуры увольнения: отзыв доступа, завершающий инструктаж. Особенности служебной документации: грифа конфиденциальности, правила хранения, передачи и уничтожения. Практическое значение: снижение человеческого фактора и повышение доверия.	ЛК, СЗ
Раздел 4	Технологии киберпреступлений и методы борьбы с ними	4.1	Основные инструменты и приемы киберпреступников	Классификация инструментов киберпреступников (вредоносное ПО, средства удаленного доступа, сканеры уязвимостей). Вредоносное программное обеспечение (вирусы, черви, трояны, шпионское ПО, программы-вымогатели). Средства анализа и разведки (сбор информации об инфраструктуре, социальные сети, OSINT). Инструменты для проникновения (бэкдоры, эксплойты, снифферы, перехватчики трафика). Приемы сокрытия следов. Методы распространения (зараженные вложения, компрометация сайтов, съемные носители). Практическое значение: знание тактик и инструментов противника для выстраивания эффективной защиты.	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
		4.2	Методы «социальной инженерии». Фишинг.	Определение социальной инженерии как манипуляции людьми для получения доступа или информации. Основные методы и приемы (подмена личности, внушение, создание срочности/страха). Использование авторитетов и должностных полномочий. Фишинг как разновидность социальной инженерии (массовые рассылки под видом легитимных организаций). Виды фишинга: обычный, целевой (spear-phishing), клонирование сайтов, поддельные формы ввода. Техническая реализация фишинговых атак (подделка отправителя, фишинговые домены, SSL-сертификаты). Признаки фишинга. Методы искусственного интеллекта для организации и обнаружения фишинга. Практическое значение: обучение персонала распознаванию и противодействию социальной инженерии.	ЛК, СЗ
		4.3	Современные и перспективные подходы к предотвращению киберпреступлений.	Переход от реактивной к проактивной модели защиты. Threat Intelligence (разведка угроз) и обмен информацией об атаках в реальном времени. Использование искусственного интеллекта и машинного обучения для обнаружения аномалий. Технологии поведенческого анализа пользователей и устройств (UEBA). Безопасная разработка (DevSecOps, автоматизированное тестирование, контроль зависимостей). Перспективные методы аутентификации (биометрия, поведенческая аутентификация). Автоматизация реагирования на инциденты (SOAR, выполнение сценариев). Практическое значение: построение адаптивной, интеллектуальной и упреждающей системы защиты.	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	Аудитория для проведения занятий лекционного типа, оснащенная комплектом специализированной мебели; доской (экраном) и техническими средствами мультимедиа презентаций.	Компьютер/ноутбук, доступ к ЭБС РУДН, MS Office, Яндекс Телемост или аналог
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, доступ к ЭБС РУДН, MS Office, Яндекс Телемост или аналог
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.	Компьютер/ноутбук, доступ к ЭБС РУДН, MS Office, Яндекс Телемост или аналог

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

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

2. Мельников, С.Ю. Искусственный интеллект и кибербезопасность : учебное пособие / С. Ю. Мельников. — Москва : Российский университет дружбы народов им. Патриса Лумумбы, 2023. — 71 с. — ISBN 978-5-209-11763-6

Дополнительная 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]

2. 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].

3. 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]

4. 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.

5. 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 «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 «Анализ и показатели эффективности кибербезопасности предприятия».

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

РАЗРАБОТЧИК:

Профессор кафедры теории вероятностей и кибербезопасности		Мельников Сергей Юрьевич
Должность, БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой теории вероятностей и кибербезопасности		Самуйлов Константин Евгеньевич
Должность БУП	*Подпись*	*Фамилия И.О.*

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой теории вероятностей и кибербезопасности		Самуйлов Константин Евгеньевич
Должность, БУП	*Подпись*	*Фамилия И.О.*