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/специальности:

09.03.03 ПРИКЛАДНАЯ ИНФОРМАТИКА
(код и наименование направления подготовки/специальности)

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

ПРИКЛАДНАЯ ИНФОРМАТИКА
(наименование (профиль/специализация) ОП ВО)

2026 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Кибербезопасность предприятия» входит в программу бакалавриата «Прикладная информатика» по направлению 09.03.03 «Прикладная информатика» и изучается в 7 семестре 4 курса. Дисциплину реализует Кафедра теории вероятностей и кибербезопасности. Дисциплина состоит из 5 разделов и 15 тем и направлена на изучение современной кибербезопасности предприятия в бизнес-информатике.

Целью освоения дисциплины 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):

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 и синтез информации, применять системный подход для решения поставленных задач	УК-1.1 Знает принципы сбора, отбора и обобщения информации, методики системного подхода для решения профессиональных задач; УК-1.2 Умеет анализировать и систематизировать разнородные данные, оценивать эффективность процедур анализа проблем и принятия решений в профессиональной деятельности; УК-1.3 Владеет навыками научного поиска и практической работы с информационными источниками; методами принятия решений;
УК-10	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	УК-10.1 Знает основные понятия социально-экономических наук и правила принятия решений в различных областях жизнедеятельности; УК-10.2 Умеет обосновывать и применять основные положения и методы социально-экономических наук для принятия решений в различных областях жизнедеятельности; УК-10.3 Владеет методами для принятия экономических решений в различных областях жизнедеятельности;
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 анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ; УК-2.3 Владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах;
ОПК-1	Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и экспериментального	ОПК-1.1 Знает основы математики, физики, вычислительной техники и программирования; ОПК-1.2 Умеет решать стандартные профессиональные задачи с применением естественнонаучных и обще-инженерных знаний, методов математического анализа и моделирования; ОПК-1.3 Владеет навыками теоретического и экспериментального исследования объектов профессиональной

Шифр	Компетенция	Индикаторы достижения компетенции (в рамках данной дисциплины)
	исследования в профессиональной деятельности	деятельности;
ОПК-2	Способен использовать современные информационные технологии и программные средства, в том числе, отечественного производства, при решении задач профессиональной деятельности	ОПК-2.1 Знает современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности; ОПК-2.2 Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности; ОПК-2.3 Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности;
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	ОПК-3.1 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; ОПК-3.2 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности; ОПК-3.3 Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научно-исследовательской работе с учетом требований информационной безопасности;
ОПК-7	Способен разрабатывать алгоритмы и программы, пригодные для практического применения	ОПК-7.1 Знает основные языки программирования и работы с базами данных, операционные системы и оболочки, современные программные среды разработки информационных систем и технологий; ОПК-7.2 Умеет применять языки программирования и работы с базами данных, современные программные среды разработки информационных систем и технологий для автоматизации бизнес-процессов, решения прикладных задач различных классов, ведения баз данных и информационных хранилищ; ОПК-7.3 Владеет навыками программирования, отладки и тестирования прототипов программно-технических комплексов;
ПК-5	Администрирование прикладного и системного программного обеспечения; управление программно-аппаратными средствами информационных служб	ПК-5.1 Знает основы архитектуры, устройства и функционирования информационно-вычислительных систем; методику установки и администрирования программных систем; ПК-5.2 Умеет реализовывать техническое сопровождение информационных систем; ПК-5.3 Имеет практический опыт эксплуатации и администрирования программных информационных систем;
ПК-6	Администрирование сетевой подсистемы инфокоммуникационной системы организации	ПК-6.1 Знает основы архитектуры, устройства и функционирования сетевых подсистем инфокоммуникационной системы организации; методику настройки и администрирования сетевых подсистем инфокоммуникационной системы организации; ПК-6.2 Умеет настраивать и администрировать сетевые подсистемы инфокоммуникационной системы организации; ПК-6.3 Имеет практический опыт эксплуатации и администрирования сетевых подсистем инфокоммуникационной системы организации;

3. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОП ВО

Дисциплина «Кибербезопасность предприятия» относится к обязательной части 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 «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***
УК-10	Способен принимать обоснованные экономические решения в различных областях жизнедеятельности	Основы военной подготовки. Безопасность жизнедеятельности; Основы формальных методов описания бизнес-процессов; Введение в управление инфокоммуникациями; Основы экономики и менеджмента;	
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; Методы обучения и адаптации больших языковых моделей;	
УК-1	Способен осуществлять поиск, критический анализ и синтез информации, применять системный подход для решения поставленных задач	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); Введение в специальность; Интеллектуальные системы; Философия; Машинное обучение в телекоммуникациях; Технологии искусственного интеллекта; Интеллектуальные методы разделения сетевых ресурсов; Введение в обучение с подкреплением; Имитационное моделирование; Методы искусственного интеллекта; Основы теории систем;	Научно-исследовательская работа; Преддипломная практика;
ОПК-1	Способен применять естественнонаучные и общеинженерные знания, методы математического анализа и моделирования, теоретического и	Символьные методы математического анализа; Алгебра и аналитическая геометрия; Дискретная математика и математическая логика;	

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
	экспериментального исследования в профессиональной деятельности	Теория вероятностей и математическая статистика; Теория конечных графов; Символьные и численные методы интегрирования дифференциальных уравнений; Имитационное моделирование; Парадигмы программирования; Физика; Химия и экология окружающей среды; Линейное и нелинейное программирование; MicroPython для устройств умного дома; Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы);	
ОПК-2	Способен использовать современные информационные технологии и программные средства, в том числе, отечественного производства, при решении задач профессиональной деятельности	Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы); Архитектура компьютеров и операционные системы; Сетевые технологии; Администрирование сетевых подсистем; Имитационное моделирование; Управление ИТ-сервисами и контентом; Цифровая грамотность, технология программирования; Парадигмы программирования; Основы информационной безопасности; Пакеты символьных вычислений в профессиональной деятельности; Интеллектуальные системы; Линейное и нелинейное программирование;	
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	Основы военной подготовки. Безопасность жизнедеятельности; Основы информационной безопасности; Научно-исследовательская работа (получение первичных навыков научно-исследовательской работы);	
ОПК-7	Способен разрабатывать алгоритмы и программы, пригодные для	Реляционные базы данных; Основы Web-технологий; Алгоритмы и структуры данных;	

Шифр	Наименование компетенции	Предшествующие дисциплины/модули, практики*	Последующие дисциплины/модули, практики*
	практического применения	Имитационное моделирование; Цифровая грамотность, основы программирования; Парадигмы программирования; Пакеты символьных вычислений в профессиональной деятельности; Интеллектуальные системы; Arduino. Практическое программирование; MicroPython для устройств умного дома;	
ПК-6	Администрирование сетевой подсистемы инфокоммуникационной системы организации	Основы администрирования операционных систем; Сетевые технологии; Администрирование сетевых подсистем; Администрирование локальных сетей; Основы информационной безопасности;	
ПК-5	Администрирование прикладного и системного программного обеспечения; управление программно-аппаратными средствами информационных служб	Основы информационной безопасности; Основы администрирования операционных систем; Администрирование сетевых подсистем; Управление ИТ-сервисами и контентом; Архитектура компьютеров и операционные системы;	

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Кибербезопасность предприятия» составляет «3» 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)**
			7
Контактная работа, ак.ч.	*54*		*54*
Лекции (**ЛК**)	18		18
Лабораторные работы (**ЛР**)	0		0
Практические/семинарские занятия (**СЗ**)	36		36
Самостоятельная работа обучающихся, ак.ч.	*54*		*54*
Контроль (экзамен/зачет с оценкой), ак.ч.	*0*		*0*
Общая трудоемкость дисциплины	**ак.ч.**	***108***	*108*
	зач.ед.	***3***	*3*

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	Раздел 1. Кибернетики как наука об управлении и организации.	1.1	Объекты управления. Инструменты управления. Технологии управления.	Рассматриваются объекты управления в контексте предприятия (бизнес-процессы, персонал, информационные системы, активы, финансовые ресурсы, инфраструктура), инструменты управления (организационно-распорядительные — приказы, регламенты, должностные инструкции; экономические — бюджетирование, мотивация; социально-психологические — корпоративная культура, коммуникации) и технологии управления (системы ERP/CRM/SCM, BI-аналитика, системы управления проектами, документооборотом и информационной безопасностью). Показано, что эффективное управление строится на согласовании объектов, инструментов и технологий, обеспечивая достижение стратегических целей, контроль исполнения и адаптацию к изменениям внешней и внутренней среды.	ЛК, СЗ
		1.2	Ресурсы управления. Взаимодействие систем.	Рассматриваются ресурсы управления (информационные — данные о состоянии предприятия, показатели эффективности; человеческие — компетенции и полномочия управленцев; технические — средства связи, серверы, АРМы; финансовые — бюджет на управленческую деятельность; временные — регламенты и циклы управления), а также взаимодействие систем как процесс обмена данными и командами между различными информационными системами предприятия (ERP, CRM, SCM, BI, DLP, SIEM, Active Directory) через интеграционные шины, API, очереди сообщений или прямые соединения. Анализируются типы взаимодействия (синхронное/асинхронное, пакетное/реальное время, инициативное/реактивное), а также риски нарушения взаимодействия (рассинхронизация данных, конфликты форматов, единые точки отказа). Показано, что согласованное использование ресурсов и надёжное взаимодействие систем являются основой оперативного и стратегического управления	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				предприятием.	
		1.3	Имидж и отношения с окружением.	Рассматриваются имидж предприятия как целенаправленно формируемый образ в сознании внешних субъектов (клиентов, партнёров, регуляторов, общества), включающий репутационные характеристики, бренд, публичные коммуникации и корпоративную культуру, а также отношения с окружением — взаимодействие с заинтересованными сторонами (стейкхолдерами): поставщиками, инвесторами, органами власти, СМИ, локальными сообществами и конкурентами. Анализируются факторы, влияющие на имидж и отношения (качество продуктов, информационная открытость, соблюдение обязательств, социальная ответственность, оперативность реагирования на инциденты), а также последствия ущерба репутации (потеря лояльности, отток клиентов, санкции регуляторов, снижение капитализации). Показано, что управление имиджем и окружением требует интеграции с процессами информационной безопасности, маркетингом и связями с общественностью, особенно при возникновении кризисных ситуаций и утечек информации.	ЛК, СЗ
Раздел 2	Кибербезопасность предприятия.	2.1	Активы предприятия. Ущерб предприятия.	Рассматриваются активы предприятия как все ресурсы, имеющие ценность для организации (материальные, информационные, кадровые, нематериальные, финансовые), подлежащие идентификации, классификации и защите. Анализируются виды ущерба предприятию, которые могут быть нанесены при нарушении конфиденциальности, целостности или доступности активов: прямой финансовый ущерб (штрафы, компенсации, восстановление систем), операционный ущерб (простои, сбои бизнес-процессов), репутационный ущерб (потеря доверия клиентов и партнёров, снижение капитализации бренда), юридический ущерб (ответственность перед регуляторами, иски), а также кадровый ущерб (текучесть персонала, снижение мотивации). Показано,	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				что полноценная оценка активов и возможных ущербов является основой для управления рисками, выбора мер защиты и планирования непрерывности бизнеса.	
		2.2	Киберугрозы предприятия. Уязвимости предприятия. Кибератаки на предприятие. Цена кибератаки.	Рассматриваются киберугрозы предприятия как совокупность потенциальных опасных событий, способных нанести ущерб активам (вредоносное ПО, фишинг, DDoS, атаки на цепочки поставок, инсайдерские угрозы), а также уязвимости предприятия как слабые места, делающие возможной реализацию угроз (необновлённое ПО, ошибки конфигурации, отсутствие сегментации сети, слабые пароли, недостаточный контроль доступа, человеческий фактор). Анализируются кибератаки на предприятие как целенаправленные воздействия злоумышленников, использующие уязвимости для реализации конкретных угроз (разведка, проникновение, закрепление, поиск целей, воздействие), включая атаки на веб-приложения, взлом почтовых систем, внедрение бэкдоров, атаки с использованием социальной инженерии. Рассматривается цена кибератаки, включающая прямые потери (выкуп, восстановление систем, штрафы), косвенные потери (простои, падение производительности, потеря клиентов), репутационный ущерб, юридические издержки и затраты на усиление защиты после инцидента. Показано, что системный анализ угроз, уязвимостей, атак и их стоимости является основой для экономически обоснованного управления рисками информационной безопасности предприятия.	ЛК, СЗ
		2.3	Возможности противника по организации кибератаки.	Рассматриваются возможности противника по организации кибератаки, включающие технический арсенал (средства автоматизированного сканирования уязвимостей, эксплойты, фреймворки для постэксплуатации (Metasploit, Cobalt Strike), вредоносное ПО (бэкдоры, шифровальщики, стелс-технологии), инструменты социальной инженерии (фишинговые конструкторы, поддельные сайты), ботнеты для	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				DDoS и рассылок), организационные ресурсы (координация группы атакующих, финансирование, использование инфраструктуры — серверы управления, прокси, анонимные сети Tor/I2P), а также тактический потенциал (способность проводить разведку, выбирать время и вектор атаки, адаптироваться к защите, маскировать следы, закрепляться в сети и действовать в обход систем обнаружения). Анализируется градация противников: от одиночных хакеров до организованных групп (APT-акторов, киберпреступных синдикатов, государственных структур) с соответствующим уровнем ресурсов, терпимости к риску и целеполагания. Показано, что реалистичная оценка возможностей противника необходима для выбора адекватных мер защиты, определения приоритетов и моделирования угроз.	
Раздел 3	Контекст деятельности предприятия.	3.1	Понимание внутренних и внешних факторов деятельности предприятия.	Рассматривается понимание внутренних и внешних факторов деятельности предприятия как основа стратегического управления и обеспечения информационной безопасности. К внутренним факторам относятся организационная структура, бизнес-процессы, кадровый состав, корпоративная культура, информационные системы, активы, финансовое состояние и компетенции сотрудников. К внешним факторам — рыночная конъюнктура, действия конкурентов, требования регуляторов, законодательные изменения, технологические тренды, экономическая ситуация, действия поставщиков и подрядчиков, а также киберугрозы и активность злоумышленников. Показано, что системный анализ внутренних факторов позволяет выявить сильные и слабые стороны, а анализ внешних — возможности и угрозы, что в совокупности формирует базу для принятия решений, оценки рисков, разработки политик безопасности и адаптации предприятия к изменяющимся условиям.	ЛК, СЗ
		3.2	Понимание потребностей и ожиданий	Рассматривается понимание потребностей и ожиданий	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
			заинтересованных сторон.	заинтересованных сторон (стейкхолдеров) как ключевой элемент управления предприятием и обеспечения его устойчивости. К заинтересованным сторонам относятся внутренние (собственники, руководство, сотрудники, профсоюзы) и внешние (клиенты, партнёры, поставщики, инвесторы, регуляторы, общество, СМИ). Анализируются основные потребности и ожидания: для клиентов — качество и безопасность услуг; для регуляторов — соответствие законодательству; для сотрудников — защита персональных данных и стабильность; для инвесторов — прозрачность и минимизация рисков; для общества — социальная ответственность. Показано, что выявление, документирование и учёт этих ожиданий необходимы для построения эффективной системы управления рисками, формирования политик информационной безопасности, приоритезации защищаемых активов и поддержания доверия к предприятию.	
		3.3	Определение области действия системы менеджмента информационной безопасности.	Рассматривается определение области действия системы менеджмента информационной безопасности (СМИБ) как процесс установления границ и применимости системы управления в соответствии со стандартом ISO/IEC 27001. Область действия включает идентифицируемые активы, организационные подразделения, физические и географические объекты, бизнес-процессы, информационные системы, персонал и взаимодействия с внешними сторонами, которые должны быть охвачены контролем. При определении области учитываются внутренние и внешние факторы деятельности предприятия, потребности заинтересованных сторон, результаты оценки рисков, а также существующая организационная и функциональная модели. Правильно определённая область позволяет избежать неоправданного расширения или необоснованного сужения СМИБ, обеспечивая сосредоточение ресурсов на критических активах и процессах, и служит основой для разработки политик, процедур и аудита.	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
Раздел 4	Руководство обеспечением кибербезопасности предприятия.	4.1	Руководящая роль и обязанности руководства. Политика в области кибербезопасности. Роли, обязанности и полномочия в организации.	Рассматривается руководящая роль и обязанности руководства предприятия в области кибербезопасности, включающие формирование стратегии, выделение ресурсов, утверждение политик, демонстрацию приверженности принципам безопасности, назначение ответственных лиц, обеспечение функционирования системы менеджмента информационной безопасности и проведение периодических обзоров её эффективности. Анализируется политика в области кибербезопасности как основополагающий нормативный документ, устанавливающий цели, принципы, требования и зоны ответственности, а также определяющий подходы к управлению рисками, контролю доступа, реагированию на инциденты и непрерывности деятельности. Описываются роли, обязанности и полномочия в организации: владельцы активов, администраторы безопасности, пользователи, внутренние аудиторы, руководители подразделений, а также при необходимости — внешние консультанты. Показано, что чёткое распределение ролей, закреплённое в нормативных документах, обеспечивает подотчётность, возможность контроля и эффективную реализацию политики кибербезопасности на всех уровнях предприятия.	ЛК, СЗ
		4.2	Планирование и действия по обработке рисков и возможностей. Цели информационной безопасности и планы по их достижению.	Рассматривается планирование в системе менеджмента информационной безопасности, включающее действия по обработке рисков (принятие, снижение, разделение, избегание) и использованию возможностей (улучшение процессов, внедрение новых технологий, повышение устойчивости) на основе результатов оценки рисков и анализа контекста предприятия. Анализируются цели информационной безопасности как измеримые, конкретные, достижимые, релевантные и ограниченные во времени результаты, которые организация намерена достичь (например, снижение времени восстановления после атаки, внедрение многофакторной аутентификации для критических систем). Описываются планы	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				по достижению целей, включающие перечень мероприятий, назначенные ресурсы, сроки, ответственных лиц и критерии оценки выполнения. Показано, что согласованное планирование рисков и целей обеспечивает непрерывное улучшение СМИБ, приоритезацию инвестиций в защиту и измеримый прогресс в области кибербезопасности предприятия.	
		4.3	Обеспечение и поддержка кибербезопасности. Ресурсы. Квалификация. Взаимодействие. Документированная информация. Функционирование. Оперативное планирование и контроль кибербезопасности.	Рассматривается обеспечение и поддержка кибербезопасности как совокупность процессов предоставления необходимых ресурсов (финансовых, технических, кадровых, информационных), развития квалификации персонала через обучение, тренинги и повышение осведомлённости, организации эффективного взаимодействия между подразделениями и с внешними сторонами (контрагентами, регуляторами, CERT), а также управления документированной информацией (политики, регламенты, журналы, отчёты). Анализируется функционирование системы менеджмента информационной безопасности как реализация запланированных процессов на ежедневной основе, включая мониторинг, управление доступом, реагирование на инциденты. Описывается оперативное планирование и контроль кибербезопасности — детализация стратегических целей на конкретные периоды и задачи, назначение исполнителей, контроль выполнения, корректирующие действия и обратная связь для непрерывного улучшения. Показано, что системное сочетание обеспечения (ресурсы, компетенции, документы) и оперативного управления является основой устойчивой и адаптируемой защиты предприятия от киберугроз.	ЛК, СЗ
Раздел 5	Меры и средства кибербезопасности предприятия и цели их	5.1	Внутренняя организация деятельности по обеспечению кибербезопасности. Мобильные устройства и дистанционная	Рассматривается внутренняя организация деятельности по обеспечению кибербезопасности, включающая распределение функций между подразделениями (SOC, IT-отдел, служба	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
	применения.		работа. Кибербезопасности, связанная с персоналом. Ответственность за активы.	безопасности, внутренний аудит), регламентацию взаимодействия, подчинение руководству и периодическую отчётность. Анализируются вопросы кибербезопасности при использовании мобильных устройств и дистанционной работе (контроль доступа через VPN, шифрование данных на устройствах, политика BYOD, защита домашних сетей, мониторинг несанкционированного подключения). Рассматривается кибербезопасность, связанная с персоналом: подбор и проверка сотрудников, обучение и повышение осведомлённости, процедуры увольнения (отзыв доступа, сдача активов), противодействие инсайдерским угрозам. Описывается ответственность за активы — закрепление конкретных материальных и информационных активов за владельцами и пользователями, включая обязанности по обеспечению их сохранности, регулярной инвентаризации, соблюдению политик доступа и информированию об инцидентах. Показано, что внутренняя организация, управление мобильностью и персоналом, а также чёткая ответственность за активы формируют устойчивую основу для защиты предприятия в условиях распределённой работы и кадровых изменений.	
		5.2	Физическая безопасность и защита от воздействия окружающей среды. Резервное копирование. Мониторинг кибербезопасности предприятия. Безопасность системы связи.	Рассматривается физическая безопасность и защита от воздействия окружающей среды (контроль доступа в помещения, видеонаблюдение, системы пожаротушения, климат-контроль, защита от затопления и перепадов электропитания, бесперебойные источники питания), а также резервное копирование как процесс регулярного создания и безопасного хранения копий критических данных (определение частоты, объёмов, мест хранения (локальное, удалённое, облачное), тестирование восстановления). Анализируется мониторинг кибербезопасности предприятия — непрерывный сбор, анализ и корреляция событий безопасности (логи, сетевой трафик, системные события) с использованием SIEM, IDS/IPS, систем анализа уязвимостей и оповещений об инцидентах.	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Наименование темы		Содержание темы	Вид учебной работы*
				Рассматривается безопасность системы связи — защита каналов передачи данных (шифрование VPN, TLS), контроль маршрутизации, защита телефонных и видеоконференцсвязи, предотвращение утечек через сетевые протоколы и несанкционированных подключений к сетевой инфраструктуре. Показано, что комплексное применение физической защиты, резервного копирования, мониторинга и безопасной связи обеспечивает целостность, доступность и конфиденциальность информации на всех уровнях функционирования предприятия.	
		5.3	Непрерывности бизнеса. Соответствие законам и нормативной базе.	Рассматривается непрерывность бизнеса как способность предприятия поддерживать критически важные функции при возникновении инцидентов, сбоев или атак, включающая анализ воздействия на бизнес (BIA), разработку планов восстановления (BCP/DRP), резервирование ресурсов, регулярное тестирование планов и обучение персонала действиям в кризисных ситуациях. Анализируется соответствие законам и нормативной базе — выполнение требований законодательства в области защиты персональных данных (152-ФЗ), государственной тайны, отраслевых стандартов (Положение Банка России, приказы ФСТЭК, требования PCI DSS для платёжных систем), а также международных норм при работе с иностранными контрагентами (GDPR, SOX). Показано, что обеспечение непрерывности бизнеса и соблюдение нормативных требований являются неотъемлемыми условиями легальной и устойчивой деятельности предприятия, влияют на доверие стейкхолдеров и требуют регулярного аудита, актуализации документации и корректирующих действий при изменениях законодательства или бизнес-среды.	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 с доступом сети Интернет и электронно-образовательной среде Университета, браузер, ПО для просмотра PDF, Яндекс Телемост
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	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, Яндекс Телемост

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

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 «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 «Кибербезопасность предприятия».

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

РАЗРАБОТЧИК:

Доцент кафедры теории вероятностей и кибербезопасности		Бесчастный Виталий Александрович
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 математического моделирования и искусственного интеллекта		Малых Михаил Дмитриевич
Должность, БУП	*Подпись*	*Фамилия И.О.*