

Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ястребов Олег Александрович
Должность: Ректор
Дата подписания: 26.05.2023 17:30:30
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

ТЕХНОЛОГИИ ОБЕСПЕЧЕНИЯ КИБЕРБЕЗОПАСНОСТИ ПРЕДПРИЯТИЙ

(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)

2023 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Дисциплина «Технологии обеспечения кибербезопасности предприятий» входит в программу бакалавриата «Кибербезопасность в экономике» по направлению 38.03.05 «Бизнес-информатика» и изучается в 5 семестре 3 курса. Дисциплину реализует Кафедра прикладной информатики и теории вероятностей. Дисциплина состоит из 5 разделов и 13 тем и направлена на изучение основных концепций и методов обеспечения кибербезопасности предприятий.

Целью освоения дисциплины является получение обучающимися знаний об основных технологиях и методах управления кибербезопасностью экономических субъектов. Усвоение курса позволит принимать эффективные управленческие решения в деятельности предприятий и организаций, иных экономических субъектов в условиях растущих угроз кибербезопасности.

2. ТРЕБОВАНИЯ К РЕЗУЛЬТАТАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Освоение дисциплины «Технологии обеспечения кибербезопасности предприятий» 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-4	Способен принимать обоснованные управленческие решения в своей профессиональной деятельности	ПК-4.1 Знает языки визуального моделирования; ПК-4.2 Умеет анализировать и оценивать факторы и условия, влияющие на принятие управленческих решений; ПК-4.3 Умеет проводить оценку эффективности принятия решения в соответствии с выбранными критериями или выбранными целевыми показателями;
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; 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 «Технологии обеспечения кибербезопасности предприятий» 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 «Технологии обеспечения кибербезопасности предприятий».

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-4	Способен принимать обоснованные управленческие решения в своей профессиональной деятельности	Микроэкономика и менеджмент; Макроэкономика; Архитектура предприятия; ИТ-инфраструктура предприятия;	Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика; Рынки ИКТ и организация продаж; Электронный бизнес; Защита сетей и кибербезопасность; Искусственный интеллект и кибербезопасность; Киберполигон;
ПК-5	Способен решать задачи управления кибербезопасностью предприятий и иных экономических систем	Цифровая трансформация глобальной экономики; Дизайн мышление;	Теневая экономика; Киберполитика в международных экономических отношениях; Мировая экономика; Искусственный интеллект в бизнесе; Финансовая безопасность; Инновации в бизнесе; Защита сетей и кибербезопасность; Анализ и показатели эффективности кибербезопасности предприятия; Искусственный интеллект и кибербезопасность; Киберполигон; Бизнес-аналитика и методы принятия решений на основе Big Data; Технологии распределенного реестра Blockchain; Правовые основы кибербезопасности; Проектная практика (получение навыков организационно-управленческой и исследовательской деятельности); Преддипломная практика;

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

** - элективные дисциплины /практики

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Технологии обеспечения кибербезопасности предприятий» 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)
			5
<i>Контактная работа, ак.ч.</i>	54		54
Лекции (ЛК)	18		18
Лабораторные работы (ЛР)	0		0
Практические/семинарские занятия (СЗ)	36		36
<i>Самостоятельная работа обучающихся, ак.ч.</i>	63		63
<i>Контроль (экзамен/зачет с оценкой), ак.ч.</i>	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	Содержание раздела (темы)		Вид учебной работы*
Раздел 1	Раздел 1. Введение, основные методы обеспечения кибербезопасности	1.1	Основные определения. Классификация технологий кибербезопасности. Цели и задачи технологий кибербезопасности	ЛК, СЗ
Раздел 2	Методы криптографии для шифрования данных	2.1	Симметричное и асимметричное шифрование. Классификация криптографических алгоритмов. Определение симметричного и асимметричного шифрования. Обмен ключами для организации безопасной связи. Алгоритмы шифрования DES (3DES), AES, RSA, SEAL, IDEA, ARCFOUR(RC4), RC5, ГОСТ 28147-89, Магма, Кузнечик (ГОСТ 34.12-2018). Совместное использование симметричных и ассиметричных ключей. Сетевые протоколы, использующие шифрование: HTTPS, SSL и TLS, PPTP, IPsec, L2TP, IKEv2/Ipsec.	ЛК, СЗ
		2.2	Цифровые подписи. Обобщенная схема ЭЦП. Криптографическая хэш-функция. Хэш-функция без ключа. Хэш-функция с ключом (код аутентификации). Безопасный обмен ключами. Цифровой сертификат. Простая электронная подпись и усиленная электронная подпись. Усиленная неквалифицированная электронная подпись и усиленная квалифицированная электронная подпись (Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»)	ЛК, СЗ
Раздел 3	Технологии контроля доступа	3.1	Защита периметра. Межсетевое экранирование, NGFW, VPN, IDS/IPS, шлюзы безопасности, сервисы защиты веб-приложений WAF. Программно-конфигурируемые сети. Управление мобильностью предприятия системы управления MDM, MAM и MIM. Системы мониторинга событий безопасности (SIEM), системы анализа сетевого трафика (NTA, средства обнаружения компьютерных атак на конечных устройствах (EDR), системы учета и обработки компьютерных угроз	ЛК, СЗ
		3.2	Виртуальная частная сеть VPN. Задачи, решаемые VPN. Туннелирование в VPN. Классификация VPN по уровню модели OSI. Защита данных на канальном уровне. Организация VPN средствами протокола PPTP. Защита данных на сетевом уровне. Протокол SKIP. Протокол IPsec, L2TP/ IPsec. Организация VPN средствами СЗИ «VipNet». Защита на транспортном уровне. Организация VPN средствами протокола SSL. Организация VPN прикладного уровня средствами протокола S/MIME. Протоколы IKEv2/IPsec, OpenVPN	ЛК, СЗ
		3.3	Аутентификация и санкционирование. Идентификация первичная и вторичная, классификация технологий идентификации. Аутентификация. Однофакторная и многофакторная аутентификация, односторонняя и взаимная аутентификация, простая, усиленная и строгая аутентификация.	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
			<p>Аутентификация по многократным и однократным паролям, аутентификация по цифровому сертификату, аутентификация по ключам доступа, аутентификация по токенам. Биометрическая аутентификация: общая схема, преимущества, проблемы. Организация передачи аутентификационной информации. Семейство протоколов AAA: RADIUS, DIAMETER, TACACS+. Сетевой протокол аутентификация Kerberos. Методы протокола аутентификации EAP. Аутентификация с использованием LDAP. Аутентификация в SSL/TLS, методы аутентификации в PPTP. OpenVPN с расширенной аутентификацией. Аутентификация в интернете.</p> <p>Санкционирование доступа (авторизация), Субъекты, объекты, методы и права доступа, привилегии субъекта доступа. Дискретная (DAC) модель управления доступом, матрица доступа. Мандатная (MAC) модель управления доступом, метки доступа. Ролевая (RBAC), атрибутивная (ABAC) модели управления доступом</p>	
Раздел 4	Антивирусные технологии, аудит и мониторинг	4.1	<p>Классификация вредоносного программного обеспечения. Классификация по деструктивному воздействию, по способу заражения объекта атаки, по степени воздействия, по способу маскировки, по среде обитания вируса, по особенностям алгоритма реализации, по способу заражения файлов. Методы обнаружения. Сигнатурные методы и бессигнатурные методы. Эвристический анализ (эвристическое сканирование). Резидентные мониторы. Обнаружение изменений и аномалий. Эмуляция программного кода. Полнотекстовый анализ (инспекция) трафика, зашифрованного протоколами различного уровня</p>	ЛК
		4.2	<p>Технологии целостности систем. Средства доверенной загрузки, средства контроля целостности данных, средства контроля целостности информационной системы, средства контроля целостности программного обеспечения, включая программное обеспечение средств защиты информации, средства контроля целостности виртуальной инфраструктуры и ее конфигураций</p>	ЛК, СЗ
		4.3	<p>Межсетевые экраны. Классификация межсетевых экранов. Требования руководящих документов ФСТЭК России к межсетевым экранам. Фильтрация пакетов. Критерии и правила фильтрации. Реализация пакетных фильтров. Системы обнаружения и предотвращения вторжений IDS/IPS. Системы анализа трафика (NTA/NDR). Межсетевые экраны нового поколения (NGFW)</p>	ЛК, СЗ
		4.4	<p>Оценка защищенности систем. Понятие защищенности информационных систем. Последовательность мероприятий по анализу защищенности. Анализ защищенности внешнего периметра сети. Анализ защищенности</p>	ЛК, СЗ

Номер раздела	Наименование раздела дисциплины	Содержание раздела (темы)		Вид учебной работы*
			внутренней инфраструктуры. Оценка эффективности принимаемых мер по обеспечению безопасности информационных систем персональных данных. Оценка эффективности системы менеджмента информационной безопасности, оценка эффективности мер обеспечения ИБ, ГОСТ Р ИСО/МЭК 27004 2021. Инструментальный анализ защищенности ИС	
		4.5	Реагирование на инциденты. Системы управления инцидентами информационной безопасности. Средства автоматизированного реагирования на инциденты информационной безопасности. Принципы менеджмента инцидентов безопасности. Рекомендации по созданию Центра обеспечения безопасности	ЛК
Раздел 5	Методы управления конфигурацией системы безопасности	5.1	Система управления политикой безопасности. Понятие системы управления политикой. Архитектурная структура IETF для управления политикой безопасности. Эталонная модель управления политикой безопасности. Узел реализации политики (PEP), точка принятия решения о политике (PDP), общая служба открытых политик (COPS), Policy Repository - репозиторий политики, облегченный протокол доступа к сетевым каталогам LDAP.	ЛК
		5.2	Усиленная защита операционных систем. Управление доступом в операционных системах семейства Windows. Субъекты, объекты и права доступа. Дескриптор защиты. Дискреционный список контроля доступа. Системный список контроля доступа. Маркера доступа. Процесс проверки подлинности при входе в систему. Защита данных средствами разрешений файловой системы NTFS. Встроенные средства защиты ОС семейства Windows. Загрузчики операционных систем LILO, GRUB. Обеспечение защиты от НСД при загрузке ОС семейства Linux. Управление доступом в операционных системах семейства GNU/Linux. Файл как универсальный объект ОС. Виды файлов. Права доступа к файлам. Субъекты, объекты, методы и права доступа. UID, EUID, GID, EGID. Разведка узлов компьютерной сети и сетевых служб. Методы сканирования узлов ЛВС. Возможности утилиты nmap. Режимы открытого и скрытого сканирования. Перехват и анализ сетевого трафика с помощью утилиты tcpdump. Наблюдение и аудит в ОС Linux. Сбор информации об опасных файловых объектах. Поиск необычных и скрытых файлов и каталогов. Наблюдение за процессами и пользователями. Встроенные средства защиты ОС семейства GNU/Linux	ЛК

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

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

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Основная литература:

1. Белоус, А. И. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения : энциклопедия / А. И. Белоус, В. А. Солодуха. — Москва : Техносфера, 2021. — 482 с. — ISBN 978-5-94836-612-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/181222> (дата обращения: 21.04.2022). — Режим доступа: для авториз. пользователей

2. Ярочкин, В. И. Информационная безопасность : учебник / В. И. Ярочкин. — 5-е изд. — Москва : Академический Проект, 2020. — 544 с. — ISBN 978-5-8291-3031-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/132242> (дата обращения: 16.04.2022). — Режим доступа: для авториз. пользователей

3. Коллинз, М. Защита сетей. Подход на основе анализа данных / М. Коллинз ; перевод с английского А. В. Добровольская. — Москва : ДМК Пресс, 2020. — 308 с. — ISBN 978-5-97060-649-0. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/131682> (дата обращения: 21.04.2022). — Режим доступа: для авториз. пользователей

4. Чيو, К. Машинное обучение и безопасность : руководство / К. Чيو, Д. Фримэн ; перевод с английского А. В. Снастина. — Москва : ДМК Пресс, 2020. — 388 с. — ISBN 978-5-97060-713-8. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/131707> (дата обращения: 21.04.2022). — Режим доступа: для авториз. пользователей

5. Гродзенский, Я. С. Информационная безопасность : учебное пособие / Я. С.

Гродзенский. — Москва : Проспект, 2020. — 142 с. — ISBN 978-5-9988-0845-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/181193> (дата обращения: 16.04.2022). — Режим доступа: для авториз. пользователей

6. Нестеров, С. А. Основы информационной безопасности : учебник для спо / С. А. Нестеров. — 2-е изд., стер. — Санкт-Петербург : Лань, 2022. — 324 с. — ISBN 978-5-8114-9489-7. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/195510> (дата обращения: 21.04.2022). — Режим доступа: для авториз. пользователей

7. Тумбинская, М. В. Комплексное обеспечение информационной безопасности на предприятии : учебник / М. В. Тумбинская, М. В. Петровский. — Санкт-Петербург : Лань, 2022. — 344 с. — ISBN 978-5-8114-3940-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/207095> (дата обращения: 16.04.2022). — Режим доступа: для авториз. пользователей

Дополнительная литература:

1. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие / А. В. Душкин, О. М. Барсуков, Е. В. Кравцов, К. В. Славнов ; под редакцией А. В. Душкина. — Москва : Горячая линия-Телеком, 2018. — 248 с. — ISBN 978-5-9912-0470-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/111053> (дата обращения: 21.04.2022). — Режим доступа: для авториз. пользователей

2. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие / В. В. Бондарев. — 2-е изд. — Москва : МГТУ им. Н.Э. Баумана, 2018. — 250 с. — ISBN 978-5-7038-4899-9. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/172839> (дата обращения: 16.04.2022). — Режим доступа: для авториз. пользователей

3. Введение в информационную безопасность : учебное пособие / А. А. Малюк, В. С. Горбатов, В. И. Королев [и др.] ; под редакцией В. С. Горбатова. — Москва : Горячая линия-Телеком, 2018. — 288 с. — ISBN 978-5-9912-0160-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: <https://e.lanbook.com/book/111075> (дата обращения: 16.04.2022). — Режим доступа: для авториз. пользователей

4. Информационный портал по безопасности — URL: <https://www.securitylab.ru>

5. Интернет-портал по информационной безопасности в сети — URL: <https://safe-surf.ru>

6. ГОСТ Р 58833-2020 Защита информации. Идентификация и аутентификация. Основные положения

7. ГОСТ Р 59383—2021. Информационные технологии. Методы и средства обеспечения безопасности. Основы управления доступом

8. ГОСТ Р (проект, первая редакция) Управление инцидентами, связанными с безопасностью информации. Руководство по реагированию на инциденты в сфере информационных и компьютерных технологий (ISO/IEC 27035-3:2020, NEQ)

9. ГОСТ 34.10 – 2018 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

10. ГОСТ Р ИСО/МЭК 27004 – 2021. Информационные технологии. Методы и средства обеспечения безопасности. Менеджмент информационной безопасности. Мониторинг, оценка защищенности, анализ и оценивание (ISO/IEC 27004:2016, IDT)

11. ГОСТ Р ИСО/МЭК 27033-4 – 2021 Информационные технологии. Методы и средства обеспечения безопасности. Безопасность сетей

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 «Технологии обеспечения кибербезопасности предприятий».

* - все 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

Оценочные материалы и балльно-рейтинговая система* оценивания уровня сформированности компетенций (части компетенций) по итогам освоения дисциплины «Технологии обеспечения кибербезопасности предприятий» представлены в Приложении к настоящей Рабочей программе дисциплины.

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

РАЗРАБОТЧИК:

Доцент кафедры

Должность, БУП



Подпись

Ботвинко Анатолий

Юрьевич

Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Заведующий кафедрой

Должность БУП



Подпись

Самуйлов Константин

Евгеньевич

Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Заведующий кафедрой

Должность, БУП



Подпись

Самуйлов Константин

Евгеньевич

Фамилия И.О.