Федеральное государственное автономное образовательное учреждение высшего образования
«Российский университет дружбы народов»

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:

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)

2022 г.

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Технологии обеспечения кибербезопасности предприятий» является получение обучающимися знаний об основных технологиях и методах управления кибербезопасностью экономических субъектов. Усвоение курса позволит им 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): ПК-4; 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-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

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 «Технологии обеспечения кибербезопасности предприятий» 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 «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[1]
ПК-4	Способность принимать обоснованные управленческие решения в своей профессиональной деятельности	Архитектура предприятия ИТ-инфраструктура предприятия	Электронный бизнес Рынки ИКТ и организация продаж Защита сетей и кибербезопасность Проектная практика Преддипломная практика
ПК-5	Способность решать задачи управления кибербезопасностью предприятий и иных экономических систем	Цифровая трансформация глобальной экономики Международные платежные системы Дизайн мышление Экономическая безопасность в современных условиях	Искусственный интеллект в бизнесе Финансовая безопасность Инновации в бизнесе Защита сетей и кибербезопасность Анализ и показатели эффективности кибербезопасности предприятия Искусственный интеллект и кибербезопасность Проектная практика Преддипломная практика

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

4. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Общая трудоемкость дисциплины «Технологии обеспечения кибербезопасности предприятий» составляет 4 зачетных единицы.

Таблица 4.1. Виды учебной работы по периодам освоения ОП ВО

Вид учебной работы		**ВСЕГО,** ак.ч.	**Семестр(-ы)**
			5
Контактная работа, ак.ч.		*54*	*54*
в том числе:			
Лекции (**ЛК**)		18	18
Лабораторные работы (**ЛР**)		-	-
Практические/семинарские занятия (**СЗ**)		36	36
Самостоятельная работа обучающихся, ак.ч.		*63*	*63*
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

Наименование раздела дисциплины	**Содержание раздела (темы)**	**Вид учебной работы**[2]
Раздел 1. Введение, основные методы обеспечения кибербезопасности	Тема 1. Основные определения. Классификация технологий кибербезопасности. Цели и задачи технологий кибербезопасности.	ЛК
Раздел 2. Методы криптографии для шифрования данных	Тема 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 - заполняется только по ОЧНОЙ форме обучения: ЛК – лекции; ЛР – лабораторные работы; СЗ – семинарские занятия

Наименование раздела дисциплины	Содержание раздела (темы)	Вид учебной работы
	Тема 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	Тема 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), системы анализа сетевого трафика нового поколения (NDR), средства обнаружения компьютерных атак на конечных устройствах (EDR), системы учета и обработки компьютерных угроз (Threat Intelligence).	ЛК
	Тема 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, WireGuard.	ЛК, СЗ
	Тема 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. Аутентификация по многоразовым и одноразовым паролям,	ЛК, СЗ

Наименование раздела дисциплины	Содержание раздела (темы)	Вид учебной работы
	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. 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.	
Раздел 4. Антивирусные технологии, аудит и мониторинг	Тема 4.1. 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.	ЛК, СЗ
	Тема 4.2. 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.	ЛК

Наименование раздела дисциплины	Содержание раздела (темы)	Вид учебной работы
	Тема 4.3. 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).	ЛК, СЗ
	Тема 4.4. Оценка защищенности систем. Понятие защищенности информационных систем. Последовательность мероприятий по анализу защищенности. Анализ защищенности внешнего периметра сети. Анализ защищенности 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.	ЛК, СЗ
	Тема 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, СЗ
Раздел 5. Методы управления конфигурацией системы безопасности	Тема 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 - репозитарий политики, облегченный протокол доступа к сетевым каталогам LDAP.	ЛК, СЗ
	Тема 5.2. Усиленная защита операционных систем. Управление доступом в операционных системах семейства Windows. Субъекты, объекты и права доступа. Дескриптор защиты.	ЛК

Наименование раздела дисциплины	Содержание раздела (темы)	Вид учебной работы
	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 скрытного 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.	

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, MS Teams.
Компьютерный класс	Компьютерный класс для проведения занятий, групповых и индивидуальных консультаций, текущего контроля и	ОС Linux, VirtualBox, дистрибутив CentOS или его аналог.

Тип аудитории	Оснащение аудитории	**Специализированное учебное/лабораторное оборудование, ПО и материалы для освоения дисциплины** (при необходимости)
	промежуточной аттестации, оснащенная персональными компьютерами (в количестве ____шт.), доской (экраном) и техническими средствами мультимедиа презентаций.	Дополнительное ПО: офисный пакет MS Office или LibreOffice
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.	ОС Linux, VirtualBox, дистрибутив CentOS или его аналог. Дополнительное ПО: офисный пакет MS Office или LibreOffice

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. Чио, К. Машинное обучение и безопасность : руководство / К. Чио, 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. ГОСТР 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 «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/модуля[3]:

1. Курс лекций по дисциплине «Технологии обеспечения кибербезопасности предприятий».
2. Практические задания по дисциплине «Технологии обеспечения кибербезопасности предприятий».

3 - 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[4] оценивания уровня сформированности компетенций (части компетенций) по итогам освоения дисциплины «Технологии обеспечения кибербезопасности предприятий» представлены в Приложении к настоящей Рабочей программе дисциплины.

РАЗРАБОТЧИКИ:

Доцент кафедры прикладной информатики и теории вероятностей		А.Ю. Ботвинко
Должность, БУП	Подпись	Фамилия И.О.

РУКОВОДИТЕЛЬ БУП:

Зав. кафедрой прикладной информатики и теории вероятностей		К.Е. Самуйлов
Наименование БУП	Подпись	Фамилия И.О.

РУКОВОДИТЕЛЬ ОП ВО:

Зав. кафедрой прикладной информатики и теории вероятностей		К.Е. Самуйлов
Должность, БУП	Подпись	Фамилия И.О.

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