МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КГЭУ»)

К Г Э У

АКТУАЛИЗИРОВАНО
решением ученого совета ИЭЭ
протокол No7 от 24.03.2026

УТВЕРЖДАЮ
Директор__*ИЭЭ*_____
__Ахметова Р.В._____
«_____»_____ 20____ г.

Подписан: ФГБОУ ВО «КГЭУ», КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»
Владелец: Ахметова Римма Валентиновна, Директор института электроэнергетики и электроники,
Сертификат: 481F880026B0CE854102CB9D 0C4FB529
Действителен с 19.06.2023 по 19.06.2024

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Б1.В.ДЭ.02.04.09 Кибербезопасность в энергетике

Направление подготовки _____13.03.02 Электроэнергетика и электротехника_____

Направленность(и) * (профиль(и)) Цифровые системы автоматизации в _____электроэнергетике_____

Квалификация _____Бакалавр_____

г. Казань, 2023

Программу разработал(и):

Наименование кафедры	Должность, уч.степень, уч.звание	ФИО разработчика
ТОЭ	Доцент, к.т.н.	Вассунова Ю.Ю.

Согласование	Наименование подразделения	Дата	№ протокола	Подпись
Одобрена	ТОЭ	18.05.2023	14	_____ Зав каф. ТОЭ, д.т.н., проф. Садыков М.Ф.
Согласована	ТОЭ	18.05.2023	14	_____ Зав каф. ТОЭ, д.т.н., проф. Садыков М.Ф.
Согласована	Учебно-методический совет института ИЭЭ	30.05.2023	8	_____ Директор ИЭЭ, к.т.н., доц. Ахметова Р.В.
Одобрена	Ученый совет института ИЭЭ	30.05.2023	9	_____ Директор ИЭЭ, к.т.н., доц. Ахметова Р.В.

1. Цель, задачи и планируемые результаты обучения по дисциплине

Целью освоения дисциплины «Кибербезопасность в электроэнергетике» является получение компетенций в вопросах кибербезопасности и защиты от киеругроз, заложить методологию обеспечения кибербезопасности информационных систем и информационных ресурсов,

используемых в профессиональной деятельности

Задачами дисциплины являются: дать представление об основных видах уязвимостей современных компьютерных систем, проанализировать наиболее актуальные киберугрозы, получить практические навыки работы с методами защиты от существующих киберугроз, развить навыки самостоятельной работы с различными источниками по вопросам информационной безопасности.

Компетенции и индикаторы, формируемые у обучающихся:

Код и наименование компетенции	Код и наименование индикатора
ПК-5 Способен разрабатывать предложения по техническому перевооружению и реконструкции оборудования;	ПК-5.3. Демонстрирует знания систем кибербезопасности в электроэнергетике

2. Место дисциплины в структуре ОП

Предшествующие дисциплины (модули), практики, НИР, др. «Информационные технологии», «Программное обеспечение и программирование в профессиональной деятельности»,

Последующие дисциплины (модули), практики, НИР, др. «Цифровые системы мониторинга и управления энергообъектов», «Моделирование процессов и объектов в электроэнергетике»

3. Структура и содержание дисциплины

3.1. Структура дисциплины

Для очной формы обучения

Вид учебной работы	Всего ЗЕ	Всего часов	Семестр
			8
ОБЩАЯ ТРУДОЕМКОСТЬ ДИСЦИПЛИНЫ	3	108	108
КОНТАКТНАЯ РАБОТА*	-	33	33
АУДИТОРНАЯ РАБОТА	0,67	24	24
Лекции	0,5	18	18
Практические (семинарские) занятия			
Лабораторные работы	0,17	6	6
САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ	2,33	84	84
Проработка учебного материала	2,33	84	84
Курсовой проект	-	-	-
Курсовая работа	-	-	-

Подготовка к промежуточной аттестации		0	0
Промежуточная аттестация:			3

3.2. Содержание дисциплины, структурированное по разделам и видам занятий

Разделы дисциплины	Всего часов	Распределение трудоемкости по видам учебной работы				Формы и вид контроля	Индексы индикаторов формируемых компетенций
		лекции	лаб. раб.	пр. зан.	сам. раб.		
Раздел 1 Введение	30	6			24	ТК1	ПК-5.З, ПК-5.У, ПК-5.В
Раздел 2 Киберпреступность и кибертерроризм	26	4			22	ТК1	ПК-5.З, ПК-5.У, ПК-5.В
Раздел 3 Концепции, стандарты и методы обеспечения кибербезопасности критических инфраструктур	28	4	4		20	ТК2	ПК-5.З, ПК-5.У, ПК-5.В
Раздел 4 Кибербезопасные микросхемы как аппаратная база киберзащитных систем	24	4	2		18	ТК2	ПК-5.З, ПК-5.У, ПК-5.В
Зачет						**ОМ**	ПК-5
ИТОГО	**108**	**18**	**6**		**84**		

3.3. Содержание дисциплины

Раздел 1. Введение

Тема 1.1. Задачи кибербезопасности в автоматизированных системах. Понятие информации и информатизации, свойства информации как объекта защиты от киберугроз

Тема 1.2. Антивирусные программы. Основные направления обеспечения кибербезопасности

Тема 1.3. Основы файловой системы. Требования к системам защиты информации

Раздел 2. Киберпреступность и кибертерроризм

Тема 2.1. Кибертерроризм - определение, способы реализации кибертеракtов

Тема 2.2. Киберпреступность. Стандарты кибербезопасности.

Раздел 3. Концепции, стандарты и методы обеспечения кибербезопасности критических инфраструктур

Тема 3.1. Тенденции развития и особенности цифровизации промышленных инфраструктур

Тема 3.2. Оценка рисков безопасности в энергетических системах

Тема 3.3 Стандарты и методы обеспечения кибербезопасности электроэнергетических инфраструктур.

Раздел 4. Кибербезопасные микросхемы как аппаратная база киберзащитных систем

Тема 4.1. Кибербезопасные микросхемы.

Тема 4.2. Современные технологии контроля безопасности

3.4. Тематический план практических занятий

-

3.5. Тематический план лабораторных работ

Лабораторная работа 1. Сравнение данных с помощью хэш-функции. Создание и сохранение надежных паролей и резервное копирование данных во внешнее хранилище»

Лабораторная работа 2. Типовые сценарии процесса анализа рисков для электроэнергетической системы. Сбор и обработка информации и оценка рисков в электроэнергетической отрасли.

3.6. Курсовой проект /курсовая работа

Данный вид работы не предусмотрен учебным планом

4. Оценивание результатов обучения

Оценивание результатов обучения по дисциплине осуществляется в рамках текущего контроля и промежуточной аттестации, проводимых по балльно-рейтинговой системе (БРС).

Шкала оценки результатов обучения по дисциплине:

Код компетенции	Код индикатора компетенции	Запланированные результаты обучения по дисциплине	Уровень сформированности индикатора компетенции			
			Высокий	Средний	Ниже среднего	Низкий
			от 85 до 100	от 70 до 84	от 55 до 69	от 0 до 54
			Шкала оценивания			
			отлично	хорошо	удовлетворительно	неудовлетворительно
			зачтено			не зачтено
ПК-5	ПК-5.3	знать:				
		основные понятия и содержание технологий обеспечения кибербезопасности ,наиболее	На высоком уровне знает основные понятия и содержан	Хорошо знает основные понятия и содержание технологи	На базовом уровне знает основные понятия и содержан	Не знает основные понятия и содержание технолог

		распространенные виды киберугроз, мехинизм кибербезопасности, методы защиты персонального компьютера	ие технологий обеспечения кибербезопасности, наиболее распространенные виды киберугроз, мехинизм кибербезопасности, методы защиты персонального компьютера	й обеспечения кибербезопасности , наиболее распространенные виды киберугроз, мехинизм кибербезопасности, методы защиты персонального компьютера. Допускает неточности	ие технологий обеспечения кибербезопасности , наиболее распространенные виды киберугроз, мехинизм кибербезопасности, методы защиты персонального компьютера. Делает ошибки	ий обеспечения кибербезопасности, наиболее распространенные виды киберугроз, мехинизм кибербезопасности, методы защиты персонального компьютера
		уметь:				
		анализировать защищенность информационно-коммуникационных средств, проводить анализ информационной безопасности объектов и систем, осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности	На высоком уровне умеет анализировать защищенность информационно-коммуникационных средств, проводить анализ информационной безопасности объектов и систем, осуществлять подбор, изучение и обобщение научно-технической	На хорошем уровне умеет анализировать защищенность информационно-коммуникационных средств, проводить анализ информационной безопасности объектов и систем, осуществлять подбор, изучение и обобщение научно-технической	На базовом уровне умеет анализировать защищенность информационно-коммуникационных средств, проводить анализ информационной безопасности объектов и систем, осуществлять подбор, изучение и обобщение научно-технической	Не умеет анализировать защищенность информационно-коммуникационных средств, проводить анализ информационной безопасности объектов и систем, осуществлять подбор, изучение и обобщение научно-технической литерату

			литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности	литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности Допускает неточности	литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности Делает ошибки.	ры, нормативных и методических материалов по вопросам обеспечения кибербезопасности
		владеть:				
		способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности, методом проведения анализа информационной безопасности объектов и систем	На высоком уровне владеет способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности, методом проведения анализа информационной безопасности	На хорошем уровне владеет способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности, методом проведения анализа информационной безопасности	На базовом уровне владеет способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности, методом проведения анализа информационной безопасности	Не владеет способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности, методом проведения анализа информационной безопасности

			объектов и систем	объектов и систем. Допускает неточности	объектов и систем. Делает ошибки.	объектов и систем

Оценочные материалы для проведения текущего контроля и промежуточной аттестации приведены в Приложении к рабочей программе дисциплины.

Полный комплект заданий и материалов, необходимых для оценивания результатов обучения по дисциплине, хранится на кафедре разработчика.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Учебно-методическое обеспечение

5.1.1. Основная литература

1. Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/293009.

5.1.2.Дополнительная литература

1. Басалова, Г. В. Основы криптографии : учебное пособие / Г. В. Басалова. — 2-е изд. — Москва : ИНТУИТ, 2016. — 282 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/100302.

2. Краковский, Ю. М. Методы защиты информации : учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — Санкт-Петербург : Лань, 2021. — 236 с. — ISBN 978-5-8114-5632-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401.

3. Мельников, В. П., Информационная безопасность : учебник / В. П. Мельников, А. И. Куприянов, Т. Ю. Васильева. — Москва : КноРус, 2023. — 371 с. — ISBN 978-5-406-11960-0. — URL: https://book.ru/book/950148. — Текст : электронный.

5.2. Информационное обеспечение

5.2.1. Электронные и интернет-ресурсы

1. Курс на площадке Moodle https://lms.kgeu.ru/course/view.php?id=4674

5.2.2. Профессиональные базы данных / Информационно-справочные системы

1. Научная электронная библиотека eLIBRARY.RU http://elibrary.ru

5.2.3. Лицензионное и свободно распространяемое программное обеспечение дисциплины

1. Windows 7 Профессиональная (Pro)
2. MATLAB Academic new Product From 10 to 24 Group Licenses (per License)
3. Simulink Academic new Product From 10 to 24 Group Licenses (per License)
4. LabVIEW Professional Development System for Windows
5. Браузер Chrome
6. Adobe Flash Player
7. LMS Moodle

6. Материально-техническое обеспечение дисциплины

Наименование вида учебной работы	Наименование учебной аудитории, специализированной лаборатории	Перечень необходимого оборудования и технических средств обучения
Лекции	Учебная аудитория для проведения занятий лекционного типа	Специализированная учебная мебель, технические средства обучения, служащие для представления учебной информации большой аудитории (мультимедийный проектор, компьютер (ноутбук), экран), демонстрационное оборудование, учебно-наглядные пособия
Лабораторные работы	Компьютерный класс с выходом в Интернет _А-309__	Специализированная учебная мебель, технические средства обучения (мультимедийный проектор Vivitek 1 шт., компьютеры в комплекте с мониторами Aquarius 11 шт.), лицензионное программное обеспечение
	Компьютерный класс с выходом в Интернет В-600а	Специализированная учебная мебель на 30 посадочных мест, 30 компьютеров, технические средства обучения (мультимедийный проектор, компьютер (ноутбук), экран), видеокамеры, программное обеспечение
Самостоятельная работа	Компьютерный класс с выходом в Интернет В-600а	Специализированная учебная мебель на 30 посадочных мест, 30 компьютеров, технические средства обучения (мультимедийный проектор, компьютер (ноутбук), экран), видеокамеры, программное обеспечение
	Читальный зал библиотеки	Специализированная мебель, компьютерная техника с возможностью выхода в Интернет и обеспечением доступа в ЭИОС, экран, мультимедийный проектор, программное обеспечение

7. Особенности организации образовательной деятельности для лиц с ограниченными возможностями здоровья и инвалидов

Лица с ограниченными возможностями здоровья (ОВЗ) и инвалиды имеют возможность беспрепятственно перемещаться из одного учебно-лабораторного корпуса в другой, подняться на все этажи учебно-лабораторных корпусов, заниматься в учебных и иных помещениях с учетом особенностей психофизического развития и состояния здоровья.

Для обучения лиц с ОВЗ и инвалидов, имеющих нарушения опорно-двигательного аппарата, обеспечены условия беспрепятственного доступа во все учебные помещения. Информация о специальных условиях, созданных для обучающихся с ОВЗ и инвалидов, размещена на сайте университета www//kgeu.ru. Имеется возможность оказания технической помощи ассистентом, а также услуг сурдопереводчиков и тифлосурдопереводчиков.

Для адаптации к восприятию лицами с ОВЗ и инвалидами с нарушенным слухом справочного, учебного материала по дисциплине обеспечиваются следующие условия:

- для лучшей ориентации в аудитории, применяются сигналы оповещения о начале и конце занятия (слово «звонок» пишется на доске);
- внимание слабослышащего обучающегося привлекается педагогом жестом (на плечо кладется рука, осуществляется нерезкое похлопывание);
- разговаривая с обучающимся, педагогический работник смотрит на него, говорит ясно, короткими предложениями, обеспечивая возможность чтения по губам.

Компенсация затруднений речевого и интеллектуального развития слабослышащих обучающихся проводится путем:

- использования схем, диаграмм, рисунков, компьютерных презентаций с гиперссылками, комментирующими отдельные компоненты изображения;
- регулярного применения упражнений на графическое выделение существенных признаков предметов и явлений;
- обеспечения возможности для обучающегося получить адресную консультацию по электронной почте по мере необходимости.

Для адаптации к восприятию лицами с ОВЗ и инвалидами с нарушениями зрения справочного, учебного, просветительского материала, предусмотренного образовательной программой по выбранному направлению подготовки, обеспечиваются следующие условия:

- ведется адаптация официального сайта в сети Интернет с учетом особых потребностей инвалидов по зрению, обеспечивается наличие крупношрифтовой справочной информации о расписании учебных занятий;
- педагогический работник, его собеседник (при необходимости), присутствующие на занятии, представляются обучающимся, при этом каждый раз называется тот, к кому педагогический работник обращается;
- действия, жесты, перемещения педагогического работника коротко и ясно комментируются;
- печатная информация предоставляется крупным шрифтом (от 18

пунктов), тотально озвучивается;

- обеспечивается необходимый уровень освещенности помещений;
- предоставляется возможность использовать компьютеры во время занятий и право записи объяснений на диктофон (по желанию обучающихся).

Форма проведения текущей и промежуточной аттестации для обучающихся с ОВЗ и инвалидов определяется педагогическим работником в соответствии с учебным планом. При необходимости обучающемуся с ОВЗ, инвалиду с учетом их индивидуальных психофизических особенностей дается возможность пройти промежуточную аттестацию устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п., либо предоставляется дополнительное время для подготовки ответа.

8. Методические рекомендации для преподавателей по организации воспитательной работы с обучающимися.

Методическое обеспечение процесса воспитания обучающихся выступает одним из определяющих факторов высокого качества образования. Преподаватель вуза, демонстрируя высокий профессионализм, эрудицию, четкую гражданскую позицию, самодисциплину, творческий подход в решении профессиональных задач, в ходе образовательного процесса способствует формированию гармоничной личности.

При реализации дисциплины преподаватель может использовать следующие методы воспитательной работы:

- методы формирования сознания личности (беседа, диспут, внушение, инструктаж, контроль, объяснение, пример, самоконтроль, рассказ, совет, убеждение и др.);
- методы организации деятельности и формирования опыта поведения (задание, общественное мнение, педагогическое требование, поручение, приучение, создание воспитывающих ситуаций, тренинг, упражнение, и др.);
- методы мотивации деятельности и поведения (одобрение, поощрение социальной активности, порицание, создание ситуаций успеха, создание ситуаций для эмоционально-нравственных переживаний, соревнование и др.)

При реализации дисциплины преподаватель должен учитывать следующие направления воспитательной деятельности:

Гражданское и патриотическое воспитание:

- формирование у обучающихся целостного мировоззрения, российской идентичности, уважения к своей семье, обществу, государству, принятым в семье и обществе духовно-нравственным и социокультурным ценностям, к национальному, культурному и историческому наследию, формирование стремления к его сохранению и развитию;
- формирование у обучающихся активной гражданской позиции, основанной на традиционных культурных, духовных и нравственных ценностях российского общества, для повышения способности ответственно реализовывать свои конституционные права и обязанности;
- развитие правовой и политической культуры обучающихся, расширение конструктивного участия в принятии решений, затрагивающих их права и

интересы, в том числе в различных формах самоорганизации, самоуправления, общественно-значимой деятельности;

- формирование мотивов, нравственных и смысловых установок личности, позволяющих противостоять экстремизму, ксенофобии, дискриминации по социальным, религиозным, расовым, национальным признакам, межэтнической и межконфессиональной нетерпимости, другим негативным социальным явлениям.

Духовно-нравственное воспитание:

- воспитание чувства достоинства, чести и честности, совестливости, уважения к родителям, учителям, людям старшего поколения;
- формирование принципов коллективизма и солидарности, духа милосердия и сострадания, привычки заботиться о людях, находящихся в трудной жизненной ситуации;
- формирование солидарности и чувства социальной ответственности по отношению к людям с ограниченными возможностями здоровья, преодоление психологических барьеров по отношению к людям с ограниченными возможностями;
- формирование эмоционально насыщенного и духовно возвышенного отношения к миру, способности и умения передавать другим свой эстетический опыт.

Культурно-просветительское воспитание:

- формирование эстетической картины мира;
- формирование уважения к культурным ценностям родного города, края, страны;
- повышение познавательной активности обучающихся.

Научно-образовательное воспитание:

- формирование у обучающихся научного мировоззрения;
- формирование умения получать знания;
- формирование навыков анализа и синтеза информации, в том числе в профессиональной области.

Вносимые изменения и утверждения на новый учебный год

№ п/п	№ раздела внесения изменений	Дата внесения изменений	Содержание изменений	«Согласовано» Зав. каф. реализующей дисциплину	«Согласовано» председатель УМК института (факультета), в состав которого входит выпускающая
1	2	3	4	5	6
1					
2					
3					

Приложение к рабочей программе дисциплины

К Г Э У

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«КАЗАНСКИЙ ГОСУДАРСТВЕННЫЙ ЭНЕРГЕТИЧЕСКИЙ УНИВЕРСИТЕТ»
(ФГБОУ ВО «КГЭУ»)

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
по дисциплине

Б1.В.ДЭ.02.04.09 Кибербезопасность в энергетике

Направление подготовки 13.03.02 Электроэнергетика и электротехника

Квалификация Бакалавр
(*Бакалавр / Магистр*)

г. Казань, 2023

Оценочные материалы по дисциплине *Кибербезопасность в энергетике* , предназначенны для оценивания результатов обучения на соответствие индикаторам достижения компетенций.

Оценивание результатов обучения по дисциплине осуществляется в рамках текущего контроля (ТК) и промежуточной аттестации, проводимых по балльно-рейтинговой системе (БРС).

1.Технологическая карта

Семестр _8_

Наименование раздела	Формы и вид контроля	Рейтинговые показатели							
		I текущий контроль	Дополнительные баллы к ТК1	II текущий контроль	Дополнительные баллы к ТК2	III текущий контроль	Дополнительные баллы к ТК3	Итого	Промежуточная аттестация
Раздел 1. Введение **Раздел 2. «**Киберпреступность и кибертерроризм»	**ТК1**	**15**	**0-15**					**15-30**	**15-30**
Тест	ОМ	7							
Раздел 3. «Концепции, стандарты и методы обеспечения кибербезопасности критических инфраструктур»	**ТК2**			**15**	**0-15**			**15-30**	**15-30**
Тест	ОМ			**7**					
Защита лабораторной работы				8					
Раздел 4. «Кибербезопасные микросхемы как аппаратная база киберзащитных систем»	ТК3					**25**	**0-15**	**25-40**	**25-40**
Тест	ОМ					7			
Защита лабораторной работы						8			
Выполнение индивидуальных заданий (рефератов)						4			
Промежуточная аттестация (зачет)	**ОМ**								**0-40**
Задание промежуточной аттестации									
В письменной форме по билетам									

2. Оценочные материалы текущего контроля и промежуточной аттестации

Шкала оценки результатов обучения по дисциплине:

Код компе-тенции	Код индикатора компетенции	Заплани-рованные результаты обучения по дисциплине	Уровень сформированности индикатора компетенции			
			Высокий	Средний	Ниже среднего	Низкий
			от 85 до 100	от 70 до 84	от 55 до 69	от 0 до 54
			Шкала оценивания			
			отлично	хорошо	удовлет-ворительно	неудов-летвори-тельно
			зачтено			не зачтено
ПК-5	ПК-5.3	знать:				
		основные понятия и содержание технологий обеспечения кибербезопасности ,наиболее распространенные виды киберугроз, механизм кибербезопасности, методы защиты персонального компьютера	На высоком уровне знает основные понятия и содержание технологий обеспечения кибербезопасности, наиболее распространенные виды киберугроз, механизм кибербезопасности, методы защиты персонального компьютера	Хорошо знает основные понятия и содержание технологий обеспечения кибербезопасности , наиболее распространенные виды киберугроз, механизм кибербезопасности, методы защиты персонального компьютера. Допускает неточности	На базовом уровне знает основные понятия и содержание технологий обеспечения кибербезопасности , наиболее распространенные виды киберугроз, механизм кибербезопасности, методы защиты персонального компьютера. Делает ошибки	Не знает основные понятия и содержание технологий обеспечения кибербезопасности, наиболее распространенные виды киберугроз, механизм кибербезопасности, методы защиты персонального компьютера
		уметь:				
		анализировать защищенность информационно-коммуникационных средств, проводить анализ	На высоком уровне умеет анализировать защищенность	На хорошем уровне умеет анализировать защищенность	На базовом уровне умеет анализировать защищенность	Не умеет анализировать защищенность информационно-коммуни

		информационной безопасности объектов и систем, осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности	информационно-коммуникационных средств, проводить анализ информационной безопасности объектов и систем, осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности	информационно-коммуникационных средств, проводить анализ информационной безопасности объектов и систем, осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности Допускает неточности	информационно-коммуникационных средств, проводить анализ информационной безопасности объектов и систем, осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности Делает ошибки.	кационных средств, проводить анализ информационной безопасности объектов и систем, осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности
		владеть:				
		способностью осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасн	На высоком уровне владеет способностью осуществлять подбор, изучение и обобщение научно-техническ	На хорошем уровне владеет способностью осуществлять подбор, изучение и обобщение научно-техническ	На базовом уровне владеет способностью осуществлять подбор, изучение и обобщение научно-техническ	Не владеет способностью осуществлять подбор, изучение и обобщение научно-технической

		ости, методом проведения анализа информационной безопасности объектов и систем	ой литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности, методом проведения анализа информационной безопасности объектов и систем	ой литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности, методом проведения анализа информационной безопасности объектов и систем. Допускает неточности	ой литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности, методом проведения анализа информационной безопасности объектов и систем. Делает ошибки.	литературы, нормативных и методических материалов по вопросам обеспечения кибербезопасности, методом проведения анализа информационной безопасности объектов и систем

Оценка **«зачтено»** выставляется за выполнение *лабораторных работ в семестре; тестовых заданий; реферата.*

Оценка **«незачтено»** выставляется за слабое и неполное выполнение *лабораторных работ в семестре; тестовых заданий; контрольных работ и реферата*.

3. Перечень оценочных средств

Краткая характеристика оценочных средств, используемых при текущем контроле успеваемости и промежуточной аттестации обучающегося по дисциплине:

Наименование оценочного средства	Краткая характеристика оценочного средства	Описание оценочного средства
Реферат (Рфр)	Продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы	Темы рефератов
Отчет по лабораторной работе (ОЛР)	Выполнение лабораторной работы, обработка результатов испытаний, измерений, эксперимента. Оформление отчета, защита результатов лабораторной работы по отчету	Перечень заданий и вопросов для защиты лабораторной

		работы, перечень требований к отчету
Тест (Тест)	Система стандартизированных заданий, позволяющая автоматизировать процедуру измерения уровня знаний и умений обучающегося	Комплект тестовых заданий

4. Перечень контрольных заданий или иные материалы, необходимые для оценки знаний, умений и навыков, характеризующих этапы формирования компетенций в процессе освоения дисциплины

Пример задания

Для текущего контроля :

Проверяемая компетенция: ПК-5.3

Тест

Вопрос	*Варианты ответа*
Почему внутренние угрозы безопасности могут нанести организации еще больший ущерб, чем внешние?	1. Внутренние пользователи – более мастерские хакеры 2. Внутренние пользователи могут подключаться к инфраструктурным устройствам через Интернет 3. У внутренних пользователей прямой доступ к инфраструктурным устройствам 4. Внутренние пользователи могут получать доступ к корпоративным данным без аутентификации
Как еще называют конфиденциальность информации?	1. Доверие 2. Согласованность 3. Неприкосновенность информации 4. Точность
Какой способ используется для проверки целостности данных?	1. Резервная копия 2. Аутентификация 3. Контрольная сумма 4. Шифрование
Какой тип атаки позволяет злоумышленнику воспользоваться методом подбора пароля (brute-force)?	1. Отказ в обслуживании 2. Перехват пакетов 3. Социальная инженерия 4. Взлом пароля
Какой инструмент используется для получения списка открытых портов на сетевых устройствах?	1. Nmap 2. Tracert 3. Whois 4. Ping
Для чего предназначен руткит?	1. Для доставки рекламы без согласия пользователя 2. Для саморепликации независимо от других программ 3. Для получения привилегированного доступа к устройствам без раскрытия себя 4. Для маскировки в качестве легитимной программы

Если данные хранятся на локальном жестком диске, как лучше всего защитить их от неавторизованного доступа?	1. Двухфакторная аутентификация 2. Дублированная копия жесткого диска 3. Удаление конфиденциальных файлов 4. Шифрование данных
Каким образом надежнее всего можно предотвратить использование уязвимости в Bluetooth?	1. Всегда использовать VPN при подключении с помощью Bluetooth 2. Использовать Bluetooth только при подключении к известному SSID 3. Всегда отключать Bluetooth, когда он активно не используется. 4. Использовать Bluetooth только для подключения к другому смартфону или планшету.
Технология какого типа может предотвратить слежение вредоносным ПО за активностью пользователей, сбор персональной информации и выдачу нежелательной всплывающей рекламы на компьютере пользователя?	1. Менеджер паролей 2. Межсетевой экран 3. Антишпионское ПО 4. Двухфакторная аутентификация
Какой тип атаки способен прерывать оказание услуг, переполняя сетевые устройства поддельным трафиком?	1. Сканирование портов 2. DDoS 3. Атака нулевого дня 4. Метод грубой силы

Отчет по лабораторной работ

Вопросы для защиты лабораторных работ 1 и 2

1. Потребитель хотел бы распечатать фотографии, хранящиеся в облачном хранилище, используя онлайн-сервис печати третьей стороны. После успешного входа в облачную учетную запись пользователю автоматически предоставляется доступ к онлайн-сервису печати третьей стороны. Почему стала возможной такая автоматическая аутентификация?

2. Технология какого типа может предотвратить слежение вредоносным ПО за активностью пользователей, сбор персональной информации и выдачу нежелательной всплывающей рекламы на компьютере пользователя?

3. Как пользователю обезопасить себя от «подслушивания» сетевого трафика, когда он пользуется публичной точкой доступа Wi-Fi на своем ПК?

4. Какая технология позволяет сократить издержки пользователя на оборудование и техническую поддержку системы резервного копирования данных?

5. Каким образом пользователям, работающим на общем компьютере, скрыть личную историю просмотров в браузере от остальных сотрудников, которые могут пользоваться этим компьютером?

6. Какая конфигурация беспроводного маршрутизатора считается неадекватной защитой для беспроводной сети?

Требования к отчету:

Каждый студент индивидуально оформляет отчет о проделанной работе, который должен содержать:

- номер работы и ее название;
- цель работы;
- предварительное задание;
- схему эксперимента и описание ее работы;
- таблицу, выводы.

Для промежуточной аттестации:
Примерные темы рефератов:

1. Потребность в кибербезопасности
2. Угрозы безопасности: понятия, типы и техники
3. Защита данных и конфиденциальности
4. Защита организации
5. Образование и карьера в сфере информационной безопасности
6. Что такое кибервойна?
7. «Способы получения доступа к информации»
8. «Изучение понятий DoS, DDoS атак, отравление SEO»
9. Защита данных и конфиденциальности
10. «Насколько рискованно ваше поведение в Интернете»
11. «Защита организации»
12. «Лучшие практические методики по информационной безопасности»