САМАРСКИЙ ПОЛИТЕХ
Самарский университет

МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ:
Директор филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске
_____ / Г.И. Заболотни
"_____" _____ 20___ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.В.02 «Кибербезопасность и криптография»

Код и направление подготовки (специальность)	13.04.02 Электроэнергетика и электротехника
Направленность (профиль)	Цифровая трансформация и управление проектами в электроэнергетике
Квалификация	Магистр
Форма обучения	Очная
Год начала подготовки	2023
Институт / факультет	Кафедры филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске
Выпускающая кафедра	кафедра "Электроэнергетика, электротехника и автоматизация технологических процессов" (НФ- ЭЭиАТП)
Кафедра-разработчик	кафедра "Информатика и системы управления" (НФ-ИиСУ)
Объем дисциплины, ч. / з.е.	288 / 8
Форма контроля (промежуточная аттестация)	Зачет, Экзамен

Самара 2023

Б1.В.02 «Кибербезопасность и криптография»

Рабочая программа дисциплины разработана в соответствии с требованиями ФГОС ВО по направлению подготовки (специальности) **13.04.02 Электроэнергетика и электротехника**, утвержденного приказом Министерства образования и науки РФ от № 147 от 28.02.2018 и соответствующего учебного плана.

Разработчик РПД:

Доцент, кандидат педагогических наук, доцент (должность, степень, ученое звание)	Е.Н Горбачевская (ФИО)
Заведующий кафедрой	С.В. Краснов, доктор технических наук, профессор (ФИО, степень, ученое звание)

СОГЛАСОВАНО:

Председатель методического совета факультета / института (или учебно-методической комиссии)	А.А Малафеев, кандидат экономических наук, доцент (ФИО, степень, ученое звание)
Руководитель образовательной программы	Е.М. Шишков, кандидат технических наук, доцент (ФИО, степень, ученое звание)
Заведующий выпускающей кафедрой	Е.М. Шишков, кандидат технических наук, доцент (ФИО, степень, ученое звание)

Содержание

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Профессиональные компетенции			
Не предусмотрено	ПК-1 Способен участвовать в управлении проектами и цифровым развитием в сфере электроэнергетики	ПК-1.6 Использует методы обеспечения кибербезопасности	Владеть навыками использования методов обеспечения кибербезопасности и криптограции
			Знать методы обеспечения кибербезопасности и криптограции
			Уметь использовать методы обеспечения кибербезопасности и криптограции

2. Место дисциплины (модуля) в структуре образовательной программы

Место дисциплины (модуля) в структуре образовательной программы: **часть, формируемая участниками образовательных отношений**

Код компетенции	Предшествующие дисциплины	Параллельно осваиваемые дисциплины	Последующие дисциплины

ПК-1		Нейронные сети в среде R; Стратегическое управление проектами цифровой трансформации; Управление проектами в электроэнергетике; Управление рисками в проектах цифровой трансформации	Машинное обучение в электроэнергетике; Микропроцессорные устройства релейной защиты и автоматики; Планирование электроэнергетических режимов электроэнергетических систем; Подготовка к процедуре защиты и защита выпускной квалификационной работы; Производственная практика: преддипломная практика; Производственная практика: проектная практика; Управление информационной средой; Управление ресурсами и сервисами информационных технологий; Устройства телемеханики и телесигнализации; Элементы активно-адаптивной электрической сети

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Вид учебной работы	Всего часов / часов в электронной форме	1 семестр часов / часов в электронной форме	2 семестр часов / часов в электронной форме
Аудиторная контактная работа (всего), в том числе:	56	24	32
Лекции	16	8	8
Практические занятия	32	16	16
Лабораторные работы	8	0	8
Самостоятельная работа (всего), в том числе:	196	84	112
подготовка к зачету	84	84	0
подготовка к экзамену	112	0	112
Контроль	36	0	36
Итого: час	288	108	180
Итого: з.е.	8	3	5

4. Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	ЛР	ПЗ	СРС	Всего часов
1	Кибербезопасность в электроэнергетике	16	8	32	196	252
	Контроль	0	0	0	0	36
	Итого	16	8	32	196	288

4.1 Содержание лекционных занятий

№ занятия	Наименование раздела	Тема лекции	**Содержание лекции** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
1 семестр				
1	Кибербезопасность в электроэнергетике	Особенности обеспечения кибербезопасности в электроэнергетике	Актуальность кибербезопасности в электроэнергетике. Компетенций в области кибербезопасности в электроэнергетике. Понятие данных, информации. Свойства информации. Операции с данными и информацией. Основные термины: защита информации, кибербезопасность, угроза, уязвимость, риск. Задачи обеспечения кибербезопасности. Базовые принципы кибербезопасности. Уязвимости в информационных системах в электроэнергетике.	2
2	Кибербезопасность в электроэнергетике	Особенности организации кибербезопасности в электроэнергетике	Классификация защищаемой информации. Базовые принципы кибербезопасности. Существующие российские и иностранные методики и стандарты обеспечения кибербезопасности. Применение моделирования для обеспечения кибербезопасности. Основные модели кибербезопасности. Модель ISO 27000.	2
3	Кибербезопасность в электроэнергетике	Виды угроз на объектах электроэнергетики	Классификация кибер-угроз. Особенности кибер-угроз на объектах электроэнергетики. Техногенные угрозы. Внешние антропогенные угрозы. Внутренне антропогенные угрозы	2
4	Кибербезопасность в электроэнергетике	Способы обеспечения кибербезопасности	Классификация способов обеспечения кибербезопасности. Правовые средства. Организационные средства. Программные, аппаратные и алгоритмические средства. Управление рисками. Управление рисками при обеспечении безопасности объектов электроэнергетики. Методики управления рисками. Расчет экономической эффективности мер кибербезопасности.	2

			Итого за семестр:	**8**
2 семестр				
5	Кибербезопасность в электроэнергетике	Правовое обеспечение кибербезопасности	Виды законодательных мер обеспечения кибербезопасности. Виды информации по уровню доступа. Российское законодательство в области кибербезопасности. Российское законодательство в области кибербезопасности объектов электроэнергетики. Европейское законодательство в области кибербезопасности объектов электроэнергетики. Примеры противоправных действий	2
6	Кибербезопасность в электроэнергетике	Организационное обеспечение кибербезопасности на объектах электроэнергетики	Организационные средства обеспечения кибербезопасности. Задачи организационные средств безопасности на объектах электроэнергетики. Классификация организационных мер. Политики безопасности организации. Регламенты и стандарты в области организационных мер обеспечения кибербезопасности. Оценка эффективности организационных мер. Роли и права доступа	2
7	Кибербезопасность в электроэнергетике	Технические средства обеспечения кибербезопасности на объектах электроэнергетики	Классификация технических средств защиты информации. Программные средства. Контроль доступа. Резервное копирование, архивирование, уничтожение. Шифрование, VPN, сетевой экран, сканер сети и портов. Антивирусы. Комплексные системы защиты. Обеспечение защиты объектов электроэнергетики при внедрении цифровых технологий.	2
8	Кибербезопасность в электроэнергетике	Технические средства обеспечения кибербезопасности на объектах электроэнергетики	Технические меры: замки, устройства идентификация и аутентификация пользователей, защитная сигнализация, системы видеонаблюдения и т.д. Примеры на объектах электроэнергетики. Техническое обеспечение программных мер. Средства (модули) доверенной загрузки, электронный ключ, токен. Алгоритмические (криптографические меры), симметричные и асимметричные системы, хэш.	2
			Итого за семестр:	**8**
			Итого:	**16**

4.2 Содержание лабораторных занятий

№ занятия	**Наименование раздела**	**Тема лабораторного занятия**	**Содержание лабораторного занятия** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	**Количество часов / часов в электронной форме**

2 семестр				
1	Кибербезопасность в электроэнергетике	Принципы управления доступом к данным	Изучение принципов управления доступов к данным как одному из 2 основных организационных методов обеспечения кибербезопасности. Принципы управления доступом к данным через роли. Работа с облачными хранилищами данных.	2
2	Кибербезопасность в электроэнергетике	Классификация кибернетических атак на предприятия	Изучение классификации кибернетических атак и информационно-справочных систем по кибернетическим атакам. Кибернетические угрозы и уязвимости, банк данных угроз безопасности информации ФСБ РФ. Использование информационно-справочной системы «MITRE ATT&CK».	2
3	Кибербезопасность в электроэнергетике	Риск-менеджмент в кибербезопасности объектов энергетики	Изучение методов риск-менеджмента в обеспечении кибербезопасности объектов энергетики.	2
4	Кибербезопасность в электроэнергетике	Криптографические способы обеспечения кибербезопасности на основе хэширования	Изучение принципов криптографической защиты информации с помощью хэш-функций. Оценка сложности пароля. Хэш-функции. Уязвимости систем аутентификации по паролям. Использование хэш-функций для обнаружения изменений в данных.	2
Итого за семестр:				**8**
Итого:				**8**

4.3 Содержание практических занятий

№ занятия	Наименование раздела	Тема практического занятия	Содержание практического занятия (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов / часов в электронной форме
1 семестр				
1	Кибербезопасность в электроэнергетике	Примеры существующих цифровых подстанций, как инструмента цифровизации электроэнергетики	Понятие цифровой подстанции (ЦПС). Примеры реализованных объектов ЦПС в России. Примеры реализации объектов ЦПС за рубежом.	2
2	Кибербезопасность в электроэнергетике	Основные протоколы ЦПС: GOOSE, MMS, SV	Протокол MMS. Протокол GOOSE. Протокол SV.	2
3	Кибербезопасность в электроэнергетике	Большие данные в электроэнергетике	Основные положения понятия большие данные. Умная энергетика.	2
4	Кибербезопасность в электроэнергетике	Обзор применения роботизированных комплексов в электроэнергетике	Беспилотные воздушные суда. Инспекционные роботы для диагностики ЛЭП. Наземная техника. Инспекция электрических станций.	2
5	Кибербезопасность в электроэнергетике	Источники больших данных в электроэнергетике и управление ресурсами на основе больших данных	Источники больших данных в энергетической системе. Управление ресурсами энергетических компаний.	2

6	Кибербезопасность в электроэнергетике	Влияние электромагнитной совместимости и помех на обеспечение кибербезопасности на энергообъектах	Влияние естественных помех. Влияние искусственных помех. Защита от электромагнитных помех.	2
7	Кибербезопасность в электроэнергетике	Анализ киберугроз в электроэнергетике	Кибернетическая безопасность энергетической инфраструктуры. Опыт обеспечения кибербезопасности ПАО «Россети».	2
8	Кибербезопасность в электроэнергетике	Государственная тайна, персональные данные, общедоступная информация	Понятие тайны и информации. Государственная тайна. Общедоступная информация.	2
			Итого за семестр:	**16**
2 семестр				
9	Кибербезопасность в электроэнергетике	NoSQL базы данных	NoSQL базы данных. Примеры баз данных NoSQL и области их применения. Достоинства и недостатки NoSQL.	2
10	Кибербезопасность в электроэнергетике	Нормативно-технические требования к СУБД российских компаний	Система управления базой данных. Требования информационных систем к СУБД.	2
11	Кибербезопасность в электроэнергетике	Примеры кибератак на объекты энергетики	Первый случай применения кибероружия в энергетике. Обзор атак вирусных программных обеспечений. Раскрытие информации IEC 61850. Протокольный уровень. Инциденты, угрожающие непрерывности управления.	2
12	Кибербезопасность в электроэнергетике	Основные кибератаки на информационные системы предприятий и технологии защиты от них	Анализ трафика. DDoS-атака (distributed denial-of-service). Бэкдор. Внедрение вредоносного программного обеспечения (ПО). Перехват TCP/IP. Фишинг. Атака по словарю.	2
13	Кибербезопасность в электроэнергетике	Коммерческая тайна, информация для служебного пользования	Коммерческая тайна. Информация для служебного пользования.	2
14	Кибербезопасность в электроэнергетике	Стратегии ведения резервных копий. Правило 3-2-1	Стратегии ведения резервных копий. Правило 3-2-1.	2
15	Кибербезопасность в электроэнергетике	Программы для шифрования-дешифрования файлов	Алгоритмы шифрования. Программы для шифрования.	2
16	Кибербезопасность в электроэнергетике	Выбор VPN-сервисов	Необходимость использования VPN. Установка VPN на компьютер. Сравнение VPN-сервисов.	2
			Итого за семестр:	**16**
			Итого:	**32**

4.4. Содержание самостоятельной работы

Наименование раздела	**Вид самостоятельной работы**	**Содержание самостоятельной работы** (перечень дидактических единиц: рассматриваемых подтем, вопросов)	**Количество часов**
1 семестр			

Кибербезопасность в электроэнергетике	Самостоятельная работа с литературой и подготовка к зачёту	Актуальность кибербезопасности в электроэнергетике. Компетенций в области кибербезопасности в электроэнергетике. Понятие данных, информации. Свойства информации. Операции с данными и информацией. Основные термины: защита информации, кибербезопасность, угроза, уязвимость, риск. Задачи обеспечения кибербезопасности. Базовые принципы кибербезопасности. Уязвимости в информационных системах в электроэнергетике. Классификация защищаемой информации. Базовые принципы кибербезопасности. Существующие российские и иностранные методики и стандарты обеспечения кибербезопасности. Применение моделирования для обеспечения кибербезопасности. Основные модели кибербезопасности. Модель ISO 27000. Классификация кибер-угроз. Особенности кибер-угроз на объектах электроэнергетики. Техногенные угрозы. Внешние антропогенные угрозы. Внутренне антропогенные угрозы. Классификация способов обеспечения кибербезопасности. Правовые средства. Организационные средства. Программные, аппаратные и алгоритмические средства. Управление рисками. Управление рисками при обеспечении безопасности объектов электроэнергетики. Методики управления рисками. Расчет экономической эффективности мер кибербезопасности.	84
		Итого за семестр:	**84**
2 семестр			

Кибербезопасность в электроэнергетике	Самостоятельная работа с литературой и подготовка к экзамену	Виды законодательных мер обеспечения кибербезопасности. Виды информации по уровню доступа. Российское законодательство в области кибербезопасности. Российское законодательство в области кибербезопасности объектов электроэнергетики. Европейское законодательство в области кибербезопасности объектов электроэнергетики. Примеры противоправных действий. Организационные средства обеспечения кибербезопасности. Задачи организационные средств безопасности на объектах электроэнергетики. Классификация организационных мер. Политики безопасности организации. Регламенты и стандарты в области организационных мер обеспечения кибербезопасности. Оценка эффективности организационных мер. Роли и права доступа. Классификация технических средств защиты информации. Программные средства. Контроль доступа. Резервное копирование, архивирование, уничтожение. Шифрование, VPN, сетевой экран, сканер сети и портов. Антивирусы. Комплексные системы защиты. Обеспечение защиты объектов электроэнергетики при внедрении цифровых технологий. Технические меры: замки, устройства идентификация и аутентификация пользователей, защитная сигнализация, системы видеонаблюдения и т.д. Примеры на объектах электроэнергетики. Техническое обеспечение программных мер. Средства (модули) доверенной загрузки, электронный ключ, токен. Алгоритмические (криптографические меры), симметричные и асимметричные системы, хэш.	112
		Итого за семестр:	**112**
		Итого:	**196**

5. Перечень учебной литературы и учебно-методического обеспечения по дисциплине (модулю)

№ п/п	Библиографическое описание	Ресурс НТБ СамГТУ (ЭБС СамГТУ, IPRbooks и т.д.)

Основная литература		
1	Кибербезопасность объектов топливно-энергетического комплекса. Концепции, методы и средства обеспечения; Инфра-Инженерия, 2020.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||98348	Электронный ресурс
2	Криптографические методы защиты информации. Часть 1. Основы криптографии; Российский государственный гидрометеорологический университет, 2010.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||17925	Электронный ресурс
3	Криптография и безопасность сетей; Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||102017	Электронный ресурс
4	Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения; Техносфера, 2021.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||108023	Электронный ресурс
Дополнительная литература		
5	Информационная безопасность и защита информации (разделы криптография и стеганография); Издательский Дом МИСиС, 2019.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||98171	Электронный ресурс
6	Основы криптографии; Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||89455	Электронный ресурс
7	Теоретико-числовые методы в криптографии. Ч.1; Рязанский государственный радиотехнический университет, 2020.- Режим доступа: https://elib.samgtu.ru/getinfo?uid=els_samgtu||iprbooks||121800	Электронный ресурс

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

6. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения

При проведении лекционных занятий используется мультимедийное оборудование.

Организовано взаимодействие обучающегося и преподавателя с использованием электронной ин-формационной образовательной среды университета.

№ п/п	Наименование	Производитель	Способ распространения
1	MATLAB	MathWorks (Зарубежный)	Лицензионное
2	Adobe Reader	Adobe Systems (Зарубежный)	Свободно распространяемое
3	LibreOffice	The Document Foundation (Зарубежный)	Свободно распространяемое
4	5 Антивирус Kaspersky Endpoint Security	АО «Лаборатория Касперского» (Отечественный)	Лицензионное

7. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

№ п/п	Наименование	Краткое описание	Режим доступа
1	Science online	http://www.sciencemag.org	Зарубежные базы данных ограниченного доступа
2	ВИНИТИ – Всероссийский Институт научной и технической информации		Российские базы данных ограниченного доступа
3	Электронная библиотека изданий СамГТУ	http://irbis.samgtu.local/cgi-bin/irbis64r_01/cgiirbis_64.exe	Российские базы данных ограниченного доступа
4	Электронно-библиотечная система IPRbooks	http://www.iprbookshop.ru/	Российские базы данных ограниченного доступа

8. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Лекционные занятия

Учебная аудитория для проведения занятий лекционного типа, текущего контроля и промежуточной аттестации, оснащённая техническими средствами обучения, служащими для представления учебной информации большой аудитории, набор демонстрационного оборудования: экран, проектор, компьютер.

Практические занятия

Компьютерный класс – учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оборудованная специализированной мебелью, компьютерной техникой с доступом в сеть "Интернет" и электронную информационно-образовательную среду СамГТУ, магнитно-маркерной доской, комплектом лицензионного и свободно распространяемого программного обеспечения, указанного в разделе 6 настоящей рабочей программы.

Лабораторные занятия

Компьютерный класс – учебная аудитория для проведения занятий семинарского типа, курсового проектирования (выполнения курсовых работ), групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, оборудованная специализированной мебелью, компьютерной техникой с доступом в сеть "Интернет" и электронную информационно-образовательную среду СамГТУ, магнитно-маркерной доской, комплектом лицензионного и свободно распространяемого программного обеспечения, указанного в разделе 6 настоящей рабочей программы.

Самостоятельная работа

Аудитория, оснащенная компьютерной техникой с возможностью подключения к сети «Интернет» и с доступом в электронную информационно-образовательную среду СамГТУ.

9. Методические материалы

Методические рекомендации при работе на лекции

До лекции студент должен просмотреть учебно-методическую и научную литературу по теме лекции с тем, чтобы иметь представление о проблемах, которые будут разбираться в лекции.

Перед началом лекции обучающимся сообщается тема лекции, план, вопросы, подлежащие рассмотрению, доводятся основные литературные источники. Весь учебный материал, сообщаемый преподавателем, должен не просто прослушиваться. Он должен быть активно воспринят, т.е. услышан, осмыслен, понят, зафиксирован на бумаге и закреплен в памяти. Приступая к слушанию нового учебного материала, полезно мысленно установить его связь с ранее изученным. Следя за техникой чтения лекции (акцент на существенном, повышение тона, изменение ритма, пауза и т.п.), необходимо вслед за преподавателем уметь выделять основные категории, законы и определять их содержание, проблемы, предполагать их возможные решения, доказательства и выводы. Осуществляя такую работу, можно значительно облегчить себе понимание учебного материала, его конспектирование и дальнейшее изучение.

Конспектирование лекции позволяет обработать, систематизировать и лучше сохранить полученную информацию с тем, чтобы в будущем можно было восстановить в памяти основные, содержательные моменты. Типичная ошибка, совершаемая обучающимся, дословное конспектирование речи преподавателя. Как правило, при записи «слово в слово» не остается времени на обдумывание, анализ и синтез информации. Отбирая нужную информацию, главные мысли, проблемы, решения и выводы, необходимо сокращать текст, строить его таким образом, чтобы потом можно было легко в нем разобраться. Желательно оставить в рабочих конспектах поля, на которых можно будет делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. С окончанием лекции работа над конспектом не может считаться завершенной. Нужно еще восстановить отдельные места, проверить, все ли понятно, уточнить что-то на консультации и т.п. с тем, чтобы конспект мог быть использован в процессе подготовки к практическим занятиям, зачету, экзамену. Конспект лекции – незаменимый учебный документ, необходимый для самостоятельной работы.

Методические рекомендации при подготовке и работе на практическом занятии

Практические занятия по дисциплине проводятся в целях выработки практических умений и приобретения навыков в решении профессиональных задач.

Рекомендуется следующая схема подготовки к практическому занятию:

1. ознакомление с планом практического занятия, который отражает содержание предложенной темы;
2. проработка конспекта лекции;
3. чтение рекомендованной литературы;
4. подготовка ответов на вопросы плана практического занятия;
5. выполнение тестовых заданий, задач и др.

Подготовка обучающегося к практическому занятию производится по вопросам, разработанным для каждой темы практических занятий и (или) лекций. В процессе подготовки к практическим занятиям, необходимо обратить особое внимание на самостоятельное изучение рекомендованной литературы.

Работа студентов во время практического занятия осуществляется на основе заданий, которые выдаются обучающимся в начале или во время занятия. На практических занятиях приветствуется активное участие в обсуждении конкретных ситуаций, способность на основе полученных знаний находить наиболее эффективные решения поставленных проблем, уметь находить полезный дополнительный материал по тематике занятий. Обучающимся необходимо обращать внимание на основные понятия, алгоритмы, определять практическую значимость рассматриваемых вопросов. На практических занятиях обучающиеся должны уметь выполнить расчет по заданным параметрам или выработать определенные решения по обозначенной проблеме. Задания могут быть групповые и

индивидуальные. В зависимости от сложности предлагаемых заданий, целей занятия, общей подготовки обучающихся преподаватель может подсказать обучающимся алгоритм решения или первое действие, или указать общее направление рассуждений. Полученные результаты обсуждаются с позиций их адекватности или эффективности в рассмотренной ситуации.

Методические рекомендации по выполнению самостоятельной работы

Организация самостоятельной работы обучающихся ориентируется на активные методы овладения знаниями, развитие творческих способностей, переход от поточного к индивидуализированному обучению с учетом потребностей и возможностей обучающегося.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной литературой, материалами периодических изданий и Интернета является наиболее эффективным методом получения дополнительных знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала. Все новые понятия по изучаемой теме необходимо выучить наизусть и внести в глоссарий, который целесообразно вести с самого начала изучения курса.

Самостоятельная работа реализуется:

- непосредственно в процессе аудиторных занятий;
- на лекциях, практических занятиях;
- в контакте с преподавателем вне рамок расписания;
- на консультациях по учебным вопросам, в ходе творческих контактов, при ликвидации задолженностей, при выполнении индивидуальных заданий и т.д.;
- в библиотеке, дома, на кафедре при выполнении обучающимся учебных и практических задач.

Эффективным средством осуществления обучающимся самостоятельной работы является электронная информационно-образовательная среда университета, которая обеспечивает доступ к учебным планам, рабочим программам дисциплин (модулей), практик, к изданиям электронных библиотечных систем.

10. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств представлен в приложении № 1.

Приложение 1 к рабочей программе дисциплины
Б1.В.02 «Кибербезопасность и криптография»

Фонд оценочных средств
по дисциплине
Б1.В.02 «Кибербезопасность и криптография»

Код и направление подготовки (специальность)	13.04.02 Электроэнергетика и электротехника
Направленность (профиль)	Цифровая трансформация и управление проектами в электроэнергетике
Квалификация	Магистр
Форма обучения	Очная
Год начала подготовки	2023
Институт / факультет	Кафедры филиала ФГБОУ ВО "СамГТУ" в г. Новокуйбышевске
Выпускающая кафедра	кафедра "Электроэнергетика, электротехника и автоматизация технологических процессов" (НФ- ЭЭиАТП)
Кафедра-разработчик	кафедра "Информатика и системы управления" (НФ-ИиСУ)
Объем дисциплины, ч. / з.е.	288 / 8
Форма контроля (промежуточная аттестация)	Зачет, Экзамен

Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения образовательной программы

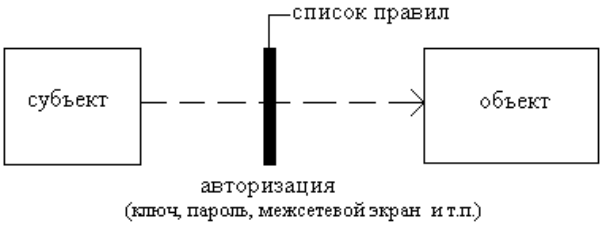
Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Профессиональные компетенции			
Не предусмотрено	ПК-1 Способен участвовать в управлении проектами и цифровым развитием в сфере электроэнергетики	ПК-1.6 Использует методы обеспечения кибербезопасности	Владеть навыками использования методов обеспечения кибербезопасности и криптографии
			Знать методы обеспечения кибербезопасности и криптографии
			Уметь использовать методы обеспечения кибербезопасности и криптографии

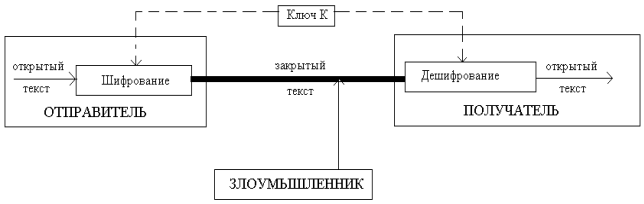
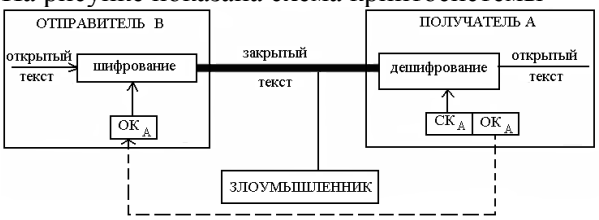
Матрица соответствия оценочных средств запланированным результатам обучения

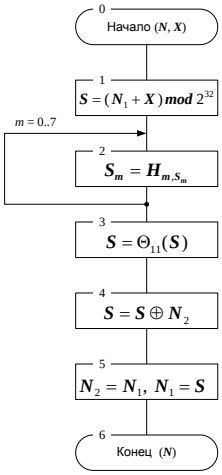
Код индикатора достижения компетенции	Результаты обучения	Оценочные средства	Текущий контроль успеваемости	Промежуточная аттестация
Кибербезопасность в электроэнергетике				
ПК-1.6 Использует методы обеспечения кибербезопасности	**Знать** методы обеспечения кибербезопасности и криптографии	Тестовые задания	Да	Да
	Владеть навыками использования методов обеспечения кибербезопасности и криптографии	Тестовые задания	Да	Да
	Уметь использовать методы обеспечения кибербезопасности и криптографии	Тестовые задания	Да	Да

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ ПО ДИСЦИПЛИНЕ
«КИБЕРБЕЗОПАСНОСТЬ И КРИПТОГРАФИЯ»
ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ
13.04.02 ЭЛЕКТРОЭНЕРГЕТИКА И ЭЛЕКТРОТЕХНИКА
(ЦИФРОВАЯ ТРАНСФОРМАЦИЯ И УПРАВЛЕНИЕ ПРОЕКТАМИ В ЭЛЕКТРОЭНЕРГЕТИКЕ)

Компетенции:
ПК-1 Способен участвовать в управлении проектами и цифровым развитием в сфере электроэнергетики.

Номер задания	Правильный ответ	Содержание вопроса	Компетенция	Номер семестра, в котором используется задание
1.	A	Выберите правильный вариант ответа. На рисунке изображена схема  **A) авторизация пользователя** B) идентификация пользователя C) аутентификация пользователя	ПК-1	1
2.	B	Выберите правильный вариант ответа. Канал утечки информации который связан с возможностью анализа злоумышленником звуковых волн, распространяющихся в воздухе, возникающих при разговоре в закрытом помещении A) электромагнитный канал **B) виброакустический канал** C) визуальный канал D) информационный канал	ПК-1	1
3.	F	Выберите правильный вариант ответа. Одним из основных принципов обеспечения информационной безопасности в АСОИ являются _____ который говорит о том, что защита не должна обеспечиваться только за счет секретности структурной организации СЗИ и алгоритмов функционирования ее подсистем. Знание алгоритма защиты не должно давать злоумышленнику возможности ее преодоления или снижать стойкость защиты A) принцип системности B) принцип комплексности C) принцип непрерывности защиты D) принцип разумной достаточности E) принцип гибкости управления и применения системы защиты **F) принцип открытости алгоритмов и механизмов защиты** G) принцип простоты применения защитных мер и средств	ПК-1	1
4.	C	Выберите правильный вариант ответа. На рисунке показана схема криптосистемы	ПК-1	1

Номер задания	Правильный ответ	Содержание вопроса	Компетенция	Номер семестра, в котором используется задание
		 A) ранцевой B) асимметричной **C) симметричной**		
5.	B	Выберите правильный вариант ответа. На рисунке показана схема криптосистемы  A) ранцевой **B) асимметричной** C) симметричной	ПК-1	1
6.	A	Выберите правильный вариант ответа. Недостатком _____ моделей политик безопасности информационных систем является их большая абстрактность, что, зачастую, не позволяет использовать правила данных моделей ко всем субъектам и объектам компьютерной системы. **A) формальных** B) неформальных	ПК-1	1
7.	D	Выберите правильный вариант ответа. Операционной системой основанной на ролевой политике безопасности, является A) OS/2 B) Unix C) Linux **D) Windows**	ПК-1	1
8.	B	Выберите правильный вариант ответа. При количественной оценке стойкости парольной защиты увеличение длины пароля приводит к _____ стойкости парольной системы защиты. A) уменьшению **B) увеличению** C) неизменности	ПК-1	1
9.	D	Выберите правильный вариант ответа. В формуле количественной оценке стойкости парольной защиты T это $$P = \frac{V * T}{S} = \frac{V * T}{A^L}$$ A) число всевозможных паролей длины	ПК-1	1

Номер задания	Правильный ответ	Содержание вопроса	Компетенция	Номер семестра, в котором используется задание
		B) длина пароля C) скорость перебора паролей злоумышленником **D) максимальный срок действия пароля**		
10.	B	Выберите правильный вариант ответа. Если символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста, то такой метод шифрование называется A) Шифрование подстановкой **B) Шифрование перестановкой** C) Шифрование гаммированием	ПК-1	1
11.	A	Выберите правильный вариант ответа. Весь алгоритм шифрования, кроме значения секретного ключа, известен криптоаналитику противника **A) правило Керхоффа** B) шифра Цезаря	ПК-1	1
12.	A	Выберите правильный вариант ответа. На рисунке изображен алгоритм  **A) алгоритм, изложенный в стандарте DES (принятый в США)** B) алгоритм шифрования принятый в РФ ГОСТом №28147-89	ПК-1	1
13.	B	Выберите правильный вариант ответа. На рисунке изображен алгоритм  A) алгоритм, изложенный в стандарте DES (принятый в США) **B) алгоритм шифрования принятый в РФ ГОСТом**	ПК-1	1

Номер задания	Правильный ответ	Содержание вопроса	Компетенция	Номер семестра, в котором используется задание
		№28147-89		
14.	A	Выберите правильный вариант ответа. В технологии ЭЦП при формировании дайжеста используют **A) функции хэширования** B) имитовставку C) гаммирование	ПК-1	1
15.	C	Выберите правильный вариант ответа. Атаки, называются также DoS-атаками (Denied of Service – отказ в обслуживании). Относятся к A) угрозам нарушения конфиденциальности информации B) угрозам нарушения целостности информации **C) угрозам нарушения работоспособности**	ПК-1	1
16.	-	Что такое Несанкционированный доступ (НСД) к информации? Ответ: Несанкционированный доступ (НСД) к информации – доступ, нарушающий установленные правила разграничения доступа. Субъект, осуществляющий НСД, является нарушителем правил разграничения доступа. НСД является наиболее распространенным видом нарушений безопасности информации.	ПК-1	2
17.	-	С точки зрения информационной безопасности выделяют следующие свойства информации: конфиденциальность, целостность и доступность. Дайте описание этим свойствам Ответ: Конфиденциальность информации – это ее свойство быть известной только допущенным и прошедшим проверку (авторизованным) субъектам системы. Для остальных субъектов системы эта информация должна быть неизвестной. Целостность информации – ее свойство быть неизменной в семантическом смысле при функционировании системы в условиях случайных или преднамеренных искажений или разрушающих воздействий. Доступность информации – ее свойство быть доступной для авторизованных законных субъектов системы, готовность служб к обслуживанию запросов.	ПК-1	2
18.	-	Перечислить принципы обеспечения информационной безопасности в информационной система **Ответ:** 1. Системности. 2. Комплексности. 3. Непрерывности защиты. 4. Разумной достаточности. 5. Гибкости управления и применения. 6. Открытости алгоритмов и механизмов защиты. 7. Простоты применения защитных мер и средств.	ПК-1	2
19.	-	Что подразумевают под ценностью информации?	ПК-1	2

Номер задания	Правильный ответ	Содержание вопроса	Компетенция	Номер семестра, в котором используется задание
		Ответ: Под ценностью информации понимается ее свойство, характеризующее потери собственника данной информации при реализации определенной угрозы, выраженные в стоимостном, временном либо ином эквиваленте		
20.	-	Перечислить меры обеспечения безопасности компьютерных систем (при классификации по способам осуществления) **Ответ:** – правовые (законодательные); – морально-этические; – организационно-административные; – физические; – аппаратно-программные.	ПК-1	2
21.	-	Перечислить *аппаратно-программным меры* защиты автоматизированных систем обработки информации **Ответ:** – идентификацию и аутентификацию субъектов АСОИ; – разграничение доступа к ресурсам АСОИ; – контроль целостности данных; – обеспечение конфиденциальности данных; – аудит событий, происходящих в АСОИ; – резервирование ресурсов и компонентов АСОИ.	ПК-1	2
22.	-	Что понимают под политикой безопасности автоматизированных систем обработки информации? **Ответ:** Под *политикой безопасности* (ПБ) понимается совокупность норм, правил и практических рекомендаций, регламентирующих процесс обработки информации, выполнение которых обеспечивает защиту от заданного множества угроз и составляет необходимое (а иногда и достаточное) условие безопасности компьютерной системы.	ПК-1	2
23.	-	Дать описание традиционной симметричной криптосистеме Ответ: В симметричных криптосистемах (криптосистемах с секретным ключом) шифрование и дешифрование информации осуществляется на одном ключе K, являющемся секретным. Рассекречивание ключа шифрования ведет к рассекречиванию всего защищенного обмена. Для того, чтобы подчеркнуть факт использования одного и того же ключа в шифраторе источника и дешифраторе получателя сообщений, криптосистемы с секретными ключами называют также одноключевыми.	ПК-1	2
24.	-	Что такое гамма шифра при шифровании методом гаммирования? **Ответ:** В *Гамма шифра* – псевдослучайная последовательность, вырабатываемая по определенному	ПК-1	2

Номер задания	Правильный ответ	Содержание вопроса	Компетенция	Номер семестра, в котором используется задание
		алгоритму, используемая для зашифровки открытых данных и дешифровки шифротекста.		
25.	-	Перечислить две основные группы методов расчёта рисков безопасности автоматизированных систем обработки информации **Ответ**: Обычно выделяют две основные группы методов расчёта рисков безопасности. Первая группа позволяет установить уровень риска путём оценки степени соответствия определённому набору требований по обеспечению информационной безопасности. Вторая группа методов оценки рисков информационной безопасности базируется на определении вероятности реализации атак, а также уровней их ущерба.	ПК-1	2
26.	-	Дайте описание принципу шифрования предложенному Шенноном **Ответ**: Принцип многоразового шифрования с помощью простых криптографических преобразований был впервые предложен Шенноном в работе: он использовал с этой целью преобразования перестановки и подстановки.	ПК-1	2
27.	-	Перечислить криптосистемы с открытым ключем **Ответ**: Наиболее известные криптосистемы с открытым ключом: • Рюкзачная криптосистема (Knapsack Cryptosystem); • Криптосистема RSA ; • Криптосистема Эль-Гамаля - EGCS (El Gamal Cryptosystem); • Криптосистема, основанная на свойствах эллиптических кривых - ECCS (Elliptic Curve Cryptosystems).	ПК-1	2
28.	-	Дать описание электронно-цифровой подписи **Ответ**: ЭЦП — это реквизит электронного документа, полученный в результате криптографического преобразования информации с использованием закрытого ключа подписи и позволяющий проверить отсутствие искажения информации в электронном документе с момента формирования подписи (целостность), принадлежность подписи владельцу сертификата ключа подписи (авторство), а в случае успешной проверки подтвердить факт подписания электронного документа (неотказуемость).	ПК-1	2
29.	-	В чем заключается шифрование перестановкой? **Ответ**: Шифрование перестановкой заключается в том, что символы открытого текста переставляются по определенному правилу в пределах некоторого блока этого текста. Данные преобразования приводят к изменению только порядка следования символов исходного сообщения.	ПК-1	2
30.	-	В чем заключается шифрование заменой?	ПК-1	2

Номер задания	Правильный ответ	Содержание вопроса	Компетенция	Номер семестра, в котором используется задание
		Ответ: Шифрование заменой (подстановкой) заключается в том, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствие с заранее оговоренной схемой замены.		
31.	-	Перечислите три типа угроз безопасности информации **Ответ:** 1. угрозы нарушения конфиденциальности информации; 2. угрозы нарушения целостности информации; 3. угрозы нарушения работоспособности системы (отказы в обслуживании).	ПК-1	2
32.	-	Что такое криптоанализ? **Ответ:** *Криптоанализ* – это наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу	ПК-1	2
33.	-	При построении стойких шифров необходимо использовать принцип рассеивания. Дайте описание принципа рассеивания **Ответ:** *Рассеивание* предполагает распространение влияния одного знака открытого текста на множество знаков шифротекста, что позволяет скрыть статистические свойства открытого текста.	ПК-1	2
34.	-	При построении стойких шифров необходимо использовать принцип перемешивания. Дайте описание принципа перемешивания **Ответ**: Перемешивание предполагает использование таких шифрующих преобразований, которые усложняют восстановление взаимосвязи статистических свойств открытого и шифротекста.	ПК-1	2
35.	-	Перечислить предложенные криптографом Ларсеном Кнудсеном методы криптоанализа блочных шифров **Ответ**: криптограф Ларс Кнудсен предлагает следующую классификацию успешных исходов криптоанализа блочных шифров в зависимости от объема и качества секретной информации, которую удалось получить: - Полный взлом - криптоаналитик извлекает секретный ключ. - Глобальная дедукция - криптоаналитик разрабатывает функциональный эквивалент исследуемого алгоритма, позволяющий зашифровывать и расшифровывать информацию без знания ключа. - Частичная дедукция - криптоаналитику удается расшифровать или зашифровать некоторые сообщения. - Информационная дедукция - криптоаналитик получает некоторую информацию об открытом тексте или ключе.	ПК-1	2
36.	-	Перечислите 4 этапа симметричного шифрования, закреплённого ГОСТом №28147-89. **Ответ**: Алгоритм предусматривает четыре режима работы: – шифрование данных в режиме простой замены; – шифрование данных в режиме гаммирования; – шифрование данных в режиме гаммирования с	ПК-1	2

Номер задания	Правильный ответ	Содержание вопроса	Компетенция	Номер семестра, в котором используется задание
		обратной связью; – выработка имитовставки.		
37.	-	Что представляет из себя имитозащита? **Ответ**: Имитозащита – это защита системы шифрованной связи от навязывания ложных сообщений, с целью обнаружения всех случайных или преднамеренных изменений в массиве информации.	ПК-1	2
38.	-	Для чего используют центры распределения ключей? **Ответ**: Обмен открытыми ключами в современных криптографических сетях, насчитывающих десятки и даже сотни тысяч пользователей более удобно реализовывать, используя специально выделенные для этого центры распределения ключей.	ПК-1	2
39.	-	Приведите примеры однонаправленных функций использующихся в криптографии Ответ: Реализация асимметричных криптосистем основана на использовании однонаправленных функций, например: Целочисленное умножение; Модульная экспонента	ПК-1	2
40.	-	Перечислите гарантии выполнения условий использования Электронно-цифровой подписи **Ответ: И**спользование ЭЦП позволяет гарантировать выполнение следующих условий. 1. Лицо или процесс, идентифицируемый как отправитель электронного документа, действительно является инициатором отправления. 2. Целостность передаваемой информации не нарушена. 3. Не дает отказаться лицу, идентифицируемого как отправителя электронного документа, от обязательств, связанных с подписанным текстом.	ПК-1	2
41.	-	Перечислите требования к функции хэширования, при формировании ЭЦП. **Ответ:** Функцией хэширования называют функцию, сжимающую сообщение произвольной длины, в значение фиксированной длины (несколько десятков или сотен бит), и обладающую свойствами необратимости, рассеивания и чувствительности к изменениям.	ПК-1	2
42.	-	Какой стандарт в РФ используют при формировании ЭЦП? **Ответ**: С 2001 года используют «КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ИНФОРМАЦИИ» ГОСТ Р 34.10-2001.	ПК-1	2
43.	-	Что понимают под цифровым сертификатом? **Ответ:** Под цифровым сертификатом понимается цифровой документ, подтверждающий соответствие открытого ключа информации, идентифицирующей владельца ключа.	ПК-1	2
44.	-	Дайте описание использованию сеансовых ключей, в	ПК-1	2

Номер задания	Правильный ответ	Содержание вопроса	Компетенция	Номер семестра, в котором используется задание
		концепции иерархии ключей при информационной защите в информационных системах. Ответ: Сеансовые ключи находятся на самом нижнем уровне и используются для шифрования данных. Когда эти ключи необходимо безопасным образом передать между узлами сети или безопасно хранить, их шифруют с помощью ключей следующего уровня		
45.	-	Опишите работу протокола одноразовых ключей S/KEY **Ответ**: Протокол одноразовых ключей S/KEY основан на независимом формировании клиентом и сервером последовательности одноразовых паролей, основанной на общем секрете K. При этом знание злоумышленником очередного пароля, пересылаемого на фазе аутентификации, не дает ему возможности выяснить следующий пароль	ПК-1	2
46.	-	Для обеспечения подлинности канала связи, и защиты от атак повторами в автоматизированных информационных системах используют метод механизм отметки времени. Дайте описание этому методу. **Ответ**: *Механизм отметки времени* заключается в том, что для каждого пересылаемого сообщения фиксируется время. Это позволяет каждому субъекту сети определить, насколько старо пришедшее сообщение, и отвергнуть его, если появится сомнение в его подлинности.	ПК-1	2
47.	-	Что представляет собой кибербезопасность? **Ответ**: Кибербезопасность (ее иногда называют компьютерной безопасностью) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных.	ПК-1	2
48.	-	Что такое кибертерроризм? **Ответ:** Кибертерроризм — комплекс незаконных действий в киберпространстве, создающих угрозу государственной безопасности, личности и обществу. Может привести к порче материальных объектов, искажению информации или другим проблемам. Основной целью кибертерроризма является влияние на решение социальных, экономических и политических задач.	ПК-1	2
49.	-	Дайте описание информационно-психологическому терроризму **Ответ**: информационно-психологический терроризм – контроль над СМИ с целью распространения дезинформации, слухов, демонстрации мощи террористических организаций; воздействие на операторов, разработчиков, представителей информационных и телекоммуникационных систем путем насилия или угрозы насилия, подкупа, введения наркотических и психотропных средств, использование методов нейролингвистического программирования, гипноза, средств создании иллюзий, мультимедийных	ПК-1	2

Номер задания	Правильный ответ	Содержание вопроса	Компетенция	Номер семестра, в котором используется задание
		средств для ввода информации в подсознание и т. д.		
50.	-	Дайте описание информационно-техническому терроризму **Ответ:** информационно-технический терроризм– нанесение ущерба отдельным физическим элементам информационной среды государства; создание помех, использование специальных программ, стимулирующих разрушение систем управления, или, наоборот, внешнее террористическое управление техническими объектами (в т. ч. самолетами), биологические и химические средства разрушения элементной базы и т. д.; уничтожение или активное подавление линий связи, неправильное адресование, искусственная перегрузка узлов коммутации и т. д.	ПК-1	2

Тестовые вопросы по дисциплине «Кибербезопасность в энергетике»

1. На что должны быть направлены меры по обеспечению информационной безопасности?
    a. **Обеспечение конфиденциальности**
    b. Обеспечение актуальности информации
    c. **Обеспечение доступности данных**
    d. **Обеспечение целостности информации**
    e. Обеспечение архивации информации

2. Что из предложенного можно назвать вредоносной программой?
    a. **Программа, выполняющая скрытый майнинг**
    b. Программа, совершающая нежелательные действия в результате ошибочных инструкций разработчика
    c. Программа анализа сетевого трафика
    d. Нелицензионное программное обеспечение
    e. Программа сканирования узлов сети

3. Что такое утечка информации?
    a. **Процесс неконтролируемого распространения информации**
    b. **Процесс раскрытия секретной информации**
    c. Процесс уничтожения информации
    d. Процесс внесения в информацию ложных сведений, приводящих к нарушению работы информационной системы
    e. Процесс перехвата сетевого трафика

4. Что можно считать несанкционированным воздействием на информацию?
    a. **Получение защищаемой информации с нарушением установленных правил**
    b. Несанкционированное подключение к внутренней WiFi сети компании
    c. **Успешная атака с целью вызвать отказ работы веб-сервисов компании**
    d. Парсинг веб-сайта компании
    e. Сканирование узлов сети компании

5. Какая категория лиц является наиболее рискованной для компании с точки зрения нарушения безопасности?
    a. **Сотрудники компании**

b. Члены семей сотрудников компании
c. Подрядчики, лица, работающие по договору
d. Злоумышленники, хакеры, криминальные структуры
e. Посетители, лица приглашенные по какому-то либо поводу

6. Какие существуют методы защиты информации?
   a. Правовые
   b. Организационные
   c. Страховые
   d. Аналитические
   e. Цифровые

7. На информационную систему компании была проведена успешная атака. Какие последствия этой атаки представляют наименьшую опасность?
   a. Получение доступа к внутренней сети компании
   b. Получение пользовательского доступа к файловому серверу
   c. Получение пользовательского доступа к персональному компьютеру рядового сотрудника
   d. Получение административного доступа к почтовому серверу компании
   e. Получение доступа к маршрутизатору сети

8. Что из перечисленного может попадать схему мошенничества фишинг?
   a. На собеседовании кандидат просит распечатать с флэшки резюме. На флэшке находится код, устанавливающий вредоносную программу
   b. Секретарю руководителя филиала компании звонит "новый директор" регионального развития. "Директор" требует срочно прислать сметы по предполагаемым конкурсам на его личную почту, поскольку в данный момент у него нет доступа к корпоративной почте
   c. **На почту приходит уведомление от популярного интернет-магазина о необходимости обновить информацию о себе. Для этого предлагается перейти по ссылке, размещенной в письме**
   d. Мошенник анализирует жесткие диски у купленных БУ компьютеров с целью поиска конфиденциальной информации
   e. Климатическую технику компании обслуживает сторонний специалист. В момент ТО кондиционера, специалист просит менеджера покинуть свое рабочее место. Менеджер уходит, оставляя компьютер не заблокированным

9. На общедоступном компьютере организации сотрудник А обнаружил, что сотрудник В не осуществил выход из своего почтового аккаунта. Какие действия сотрудника А будут являться нарушением законодательства РФ?
    a. Сотрудник А вызывает специалиста по информационной безопасности и сообщает о проблеме
    b. Сотрудник А просматривает почту, с целью определить ФИО и отдел сотрудника В, чтобы сообщить ему об оплошности
    c. Сотрудник А осуществляет выход из аккаунта сотрудника В
    d. Сотрудник А в присутствии свидетеля меняет пароль сотрудника В, чтобы предотвратить утечку информации
    e. Сотрудник А не предпринимает никаких действий

10. Пусть U – потенциально возможная величина ущерба при распространении информации, V – потенциально возможная величина выгоды при свободном распространении информации, p – вероятность проявления ущерба в период жизненного цикла информации, q – вероятность проявления выгоды в период жизненного цикла при свободном распространении информации, Z – величина затрат на защиту информации. При каком условии целесообразно отнести информацию к информации ограниченного доступа?
    a. $U*p-V*q+Z>0$
    b. $U*p-V*q+Z<0$
    c. $U*p-V*q-Z>0$
    d. $U*p-V*q-Z<0$
    e. $U*p+V*q-Z<0$

11. Что из перечисленного попадает под категорию персональных данных?
    a. Фамилия, имя, отчество
    b. Фотография на паспорт
    c. Сведения об умершем
    d. Объявление на подъезде с указанием фамилии жильца и размера его долга по оплате электроэнергии
    e. Все перечисленное
12. Что из перечисленного попадает под категорию общедоступная информация?
    a. Информация, размещенная на корпоративном сервере, доступ к которой можно получить любым субъектом из внутренней сети компании

b. **Информация, размещенная на корпоративном сервере, доступ к которой можно получить из сети Интернет**
c. Информация, размещенная на корпоративном сервере, доступ к которой можно получить субъект, обладающим необходимыми правами
d. Ничего из перечисленного

13. Какие из возможных событий, могут представлять угрозу для информационной безопасности?
    a. Информационная рассылка по организации об участившихся случаях вирусных атак и требованием соблюдать должностные инструкции
    b. **Письмо от руководителя подразделения, в котором на основании приказа по организации требуется установить критическое обновление операционной системы**
    c. **Письмо от отдела кадров с просьбой прислать паспортные данные и СНИЛС**
    d. Письмо от главного энергетика с предупреждением об отключении электричества в некотором промежутке рабочего времени
    e. Письмо рекламного характера, предлагающего скидки в крупном торговом центре вашего города

14. Сотрудником был утерян пароль к одному из сервисов компании. Какие действия допустимы с точки зрения информационной безопасности?
    a. Попросить у коллеги пароль и продолжить работу под его аккаунтом
    b. Запросить и получить по почте от специалистов технической поддержки новый пароль
    c. Лично получить от специалистов технической поддержки новый пароль на традиционном носителе, например, бумага. Уничтожить носитель после сохранения в надежном месте пароля
    d. **Ни один из предложенных вариантов**

15. Какие меры будут наиболее эффективны для снижения ущерба от стихийных явлений?
    a. Программные
    b. Законодательные
    c. **Организационные**
    d. Криптографические
    e. Стеганографические

16. Как называется операция по предоставлению определенному лицу или кругу кругу лиц прав на выполнение некоторых действий?
    a. Авторизация
    b. Аутентификация
    c. Идентификация
    d. Указание
    e. Спецификация

17. Что из предложенного подходит под описание двухфакторной аутентификации?
    a. Необходимость дважды предоставить системе пароль, аутентификация считается выполненной в случае их совпадения
    b. Необходимость дважды предоставить системе логин и пароль. Первый раз при входе в систему, второй раз через некоторый промежуток времени
    c. Необходимость предоставить системе PIN код и отпечаток пальца
    d. Необходимость при регистрации указывать резервный почтовый ящик

18. Выберите сервисы повышающие уровень безопасности.
    a. Идентификация и аутентификация
    b. Структуризация хранимой информации
    c. Кэширование обрабатываемой информации
    d. Сжатие передаваемых данных
    e. Протоколирование и аудит

19. Что из перечисленного является наиболее эффективным средством от сетевых атак?
    a. Применение фаервола
    b. Применение антивирусных программ
    c. Журналирование действий пользователя в сети
    d. Посещение только «надёжных» Интернет-узлов
    e. Использование сертифицированных браузеров при доступе к сети Интернет

20. С какой целью применяются DLP-системы (системы предотвращения утечек)?

a. Блокирование пересылаемой информации на основе правил протокол\хост\порт
b. Вычисление сотрудников, планирующих смену работы, для минимизации риска утечки данных вместе с увольняющимися кадрами
c. Поиск вирусов в файлах пересылаемых в мессенджерах
d. Анализ содержимого электронных писем
e. Анализ открытых портов на узлах сети, где установлен клиент DLP-системы

21. Какие задачи стоят перед системой обнаружения вторжений?
a. Поиск атак направленных на повышение привилегий
b. Задачи аналогичные межсетевому экрану, но работа системы ведется на уровне узла сети
c. Идентификация пользователей на основе их биометрических данных
d. Анализ трафика на совпадение с сигнатурами атаки
e. Анализ данных с видеокамер отслеживающих перемещение персонала компании на охраняемой территории

22. Что из перечисленного будет определено антивирусным ПО как троянская вирусная программа?
a. Вредоносная программа, распространяющаяся самостоятельно, путем перемещения своей копии с одного носителя на другой
b. Вредоносная программа, ссылку на которую пользователь получил в письме как бесплатное ПО с некоторым полезным функционалом
c. Вредоносная программа, распространяющаяся через локальную сеть, используя ошибки администрирования
d. Вредоносная программа, способная внедрять свой код в тело других программ

23. Какие из перечисленных мер можно отнести к аппаратно-техническим мерам защиты информации?
a. Пожарная сигнализация
b. Регламент использования корпоративной информационной системы
c. Трудовые соглашения, определяющие ответственность сотрудников
d. Биометрическая система аутентификации пользователей
e. Регламент доступа в серверное помещение

24. Какие из перечисленных мер можно рекомендовать для обеспечения целостности базы данных?
    a. Применение технологий предотвращения утечек информации
    b. Применение межсетевого экрана
    c. Применение технологий резервного копирования
    d. Применение некоторых технологий RAID (избыточный массив дисков), например RAID 1 или RAID 5
    e. Определение в политике безопасности запрет подключения к базе данных извне, введение требований к сложности паролей пользователей базы данных

25. Какой из предложенных способов можно рекомендовать для защиты программного обеспечения от несанкционированного распространения?
    a. Антивирусное программное обеспечение
    b. Электронный (аппаратный) ключ
    c. Межсетевой экран
    d. Средства уничтожения носителей информации
    e. Система обнаружения вторжений

26. С какой целью применяется аппаратный токен?
    a. Устройство, для удаления информации в случае ее кражи
    b. Устройство, применяемое для поиска утерянной мобильной техники
    c. Устройство, используемое для упрощения аутентификации
    d. Устройство, для поиска вредоносных программ

27. Каковы возможности межсетевого экрана?
    a. Повышение пропускной способности сети
    b. Защита от вирусов и спама
    c. Разрешение трафика согласно указанным правилам
    d. Запрет трафика согласно указанным правилам
    e. Шифровка/расшифровка передаваемой информации

28. С какой целью можно использовать хэш-функции?
    a. Для хранения паролей
    b. Для шифрования/расшифрования информации на жестком диске
    c. Для расчета контрольных сумм при передаче данных
    d. Для шифрования/расшифрования информации передаваемой по открытым каналам связи
    e. Для проверки зашифрованного сообщения на криптостойкость

29. Что является слабым местом симметричного шифрования?
    a. Это устаревшие способы шифрования, в настоящий момент не используются
    b. Медлительные и трудоемкие методы шифрования, требующие существенных вычислительных мощностей
    c. Существует проблема передачи ключа шифрования между источником и приемником данных
    d. Необходимость наличия двух ключей, что увеличивает вероятность утечки информации

30. Что из приведенного можно отнести к достоинствам методов асимметричного шифрования?
    a. Возможность отправлять ключ для шифрования данных по открытым каналам связи
    b. Низкие требования к вычислительным мощностям при шифровании и расшифровании
    c. Увеличение скорости передачи данных за счет сжатия информации при шифровании
    d. Малая длина ключа за счет чего обеспечивается высокая скорость шифрования и расшифрования
    e. Возможность обходиться без ключей шифрования

31. Какие функции может обеспечить электронная подпись?
    a. Конфиденциальную связь
    b. Исключение отказа от сообщения
    c. Подлинность сообщения
    d. Целостность сообщения
    e. Актуальность сообщения

32. Каким основным стандартом регламентируется информационный обмен устройств релейной защиты цифровых подстанций?
    a. МЭК-61850
    b. МЭК-61131
    c. ПУЭ
    d. СНИП

33. Для обеспечения надежности и живучести цифровых подстанций применяют
    a. Дублирование функций

b. Дублирование устройств
c. Дублирование ЛВС и каналов связи
d. Всё вышеперечисленное

34. Основные требования к передаче мгновенных значений тока и напряжения по шине процесса:
a. Выполнение дискретизации аналоговых сигналов с высокой частотой для обеспечения корректной работы алгоритмов РЗА.
b. Обеспечение минимальной задержки при передаче данных в реальном времени, а также синхронизация измерений по времени.
c. Передаются только действующие значения промышленной частоты
d. Обеспечение возможности выявления потерь и искажений данных при их передаче

35. Выберите одно наиболее верное определение цифровой трансформации:
a. автоматизация обработки данных в цифровом формате
b. компьютеризация производственных процессов
c. создание новых бизнес-моделей и процессов путем внедрения цифровых технологий
d. замена аналогового способа передачи данных на цифровой

36. Выберите две наиболее важные технологии Индустрии 4.0 из перечисленных:
a. кибер-физические системы
b. беспроводная передача данных
c. автопилоты
d. искусственный интеллект
e. 3D-печать

37. Выберите верные утверждения:
a. термины цифровизация и информатизация - синонимы
b. термины цифровизация и информатизация имеют принципиальные отличия
c. термины цифровизация и компьютеризация – синонимы
d. термины цифровизация и автоматизация имеют принципиальные отличия

38. Что содержит Электронный эксплуатационный паспорт оборудования согласно проекту (выберите один вариант)?

a. **характеристики оборудования, историю эксплуатации и документацию (схемы, чертежи)**
b. характеристики оборудования и документацию (схемы, чертежи)
c. только паспортные данные оборудования
d. только идентификатор оборудования и историю эксплуатации
e. характеристики оборудования и документацию (схемы, чертежи)

39. Укажите технологии, которые относятся к Промышленному Интернету вещей:
a. **радиочастотная идентификация (RFID)**
b. накопители энергии
c. **цифровые двойники**
d. **технологии высокоскоростного беспроводного обмена данными**
e. аналоговые компьютеры

40. Выберите примеры, которые можно отнести к применению технологии Промышленного Интернета вещей в энергетике:
a. создание прикладного программного обеспечения для расчета режимов электрической сети
b. **создание цифрового двойника силового трансформатора**
c. внедрение корпоративной информационной системы на предприятии ТЭК
d. **создание прикладного программного обеспечения для интеллектуальной диагностики состояния электрооборудования по собираемым с него данным**

41. Что включает в себя правовая защита информации (выберите один вариант)?
a. разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации и применение этих документов (актов)
b. **разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением**
c. криптографическое преобразование информации в соответствии с нормативными правовыми документами (актами)
d. применение технических, аппаратных и криптографических средств защиты информации

42. Что подразумевает по собой физическая защита информации (выберите один вариант)?
    a. **применение средств создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты**
    b. разработку организационных мероприятий для предотвращения несанкционированного доступа к информации
    c. защиту информации на материальных носителях на территории охраняемого объекта
    d. все перечисленное

43. Что может быть отнесено к объектам защиты информации согласно Национальному стандарту РФ “Защита информации”?
    a. сотрудник предприятия
    b. территория
    c. здание (сооружение)
    d. выделенное помещение
    e. электроэнергетическая установка
    f. информация

44. Согласно Национальному стандарту РФ “Защита информации” защищать информацию можно от (возможно несколько вариантов ответа):
    a. утечки
    b. искажения
    c. потери
    d. непреднамеренного воздействия
    e. иностранной разведки
    f. кражи

45. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности - это (выберите один вариант):
    a. политика безопасности информации в организации
    b. система защиты информации
    c. регламент защиты информации
    d. политика и система безопасности информации в организации

46. Кто может быть собственником информации (выберите один вариант)?
    a. государство, юридическое лицо, группа физических лиц, но не отдельное физическое лицо
    b. государство, юридическое лицо, группа физических лиц, отдельное физическое лицо

c. юридическое лицо, группа физических лиц, отдельное физическое лицо, но не государство
d. только государство или юридическое лицо

47. Что может быть носителем защищаемой информации (выберите один вариант)?
    a. только материальный объект
    b. материальный или виртуальный (цифровой объект)
    c. только физическое лицо
    d. физическое лицо или материальный объект

48. Свойство информационной системы, обусловливающее возможность реализации угроз безопасности обрабатываемой в ней информации - это (выберите один вариант):
    a. уязвимость
    b. проблема безопасности информационной системы
    c. угроза
    d. опасность нарушения безопасности данных

49. Укажите наиболее правильное определение термина «Большие данные» (Big Data):
    a. данные очень большого объема и технологии их интеллектуального анализа
    b. неоднородные данные, которые поступают с большой скоростью
    c. неоднородные данные большого объема, которые поступают с высокой скоростью и технологии их обработки
    d. под Big Data подразумевают или только сами данные, имеющие высокую степень многообразия, большие объем и скорость поступления; или кроме данных подразумевают еще и технологии работы с ними

50. Что подразумевает термин «цифровая подстанция» (возможно несколько вариантов ответа)?
    a. замену электромеханических реле на микропроцессорные терминалы с передачей цифровых сигналов
    b. подстанцию с широким применением стандарта МЭК-61850 и обменом данными преимущественно в цифровом формате
    c. подстанцию с любой системой АСУ ТП
    d. цифровой двойник реальной подстанции

51. Что такое локальная вычислительная сеть (выберите один вариант)?

a. **единая, интегрированная, иерархическая распределенная человеко-машинная система, оснащенная средствами управления, измерения, сбора, обработки, отображения, регистрации, хранения и передачи информации**
b. общая сеть обмена данными между элементами информационной системы
c. единая, децентрализованная компьютерная система, оснащенная средствами управления, измерения, сбора, обработки, отображения, регистрации, хранения и передачи информации
d. единая иерархическая система взаимосвязанных и взаимодействующих вычислительных машин, оснащенная средствами управления, измерения, сбора, обработки, отображения, регистрации, хранения и передачи информации

52. На каком уровне располагается автоматизированное рабочее место (АРМ) в структуре ЦПС?
a. процесса
b. присоединения
c. подстанции
d. АРМ не входит в структуру ЦПС

53. На каком уровне располагаются интеллектуальные электронные устройства, выполняющие функции РЗА, в структуре ЦПС?
a. процесса
b. присоединения
c. подстанции
d. процесса или подстанции

54. Укажите основные отличия цифровых подстанций от традиционных:
a. процессы информационного обмена между элементами ПС осуществляются преимущественно в цифровом виде
b. управление работой ПС осуществляются в цифровом виде
c. организация информационного обмена согласно МЭК-61850
d. наличие АСУ ТП

55. Какие существуют препятствия для внедрения ЦПС?
a. экономический эффект не всегда очевиден
b. нехватка специалистов
c. риски угроз со стороны кибератак

d. ничего из перечисленного

56. Согласно национальному профилю ПАО ФСК ЕЭС какая форма передачи сигналов должна преобладать на цифровой подстанции:
    a. ццифровая, посредством Wi-Fi
    b. цифровая, посредством оптических и/или Ethernet кабелей
    c. аналоговая, посредством медных контрольных кабелей
    d. аналоговая, посредством 3G

57. Программа, предназначенная для осуществления несанкционированного доступа к информации и (или) воздействия на информацию или ресурсы информационной системы - это (выберите один вариант):
    a. вирус
    b. вредоносная программа
    c. киберугроза
    d. программа-взломщик

58. Средства защиты информации, основанные на ее шифровании, относятся к (выберите один вариант):
    a. физическим средствам защиты
    b. аппаратным средствам защиты
    c. криптографическим средствам защиты
    d. правовым средствам защиты

59. Эффективность защиты информации - это (выберите один вариант):
    a. степень соответствия результатов защиты информации цели защиты информации
    b. степень использования всех средств защиты информации
    c. степень соответствия результатов защиты информации принятым в организации стандартам
    d. величина, обратно-пропорциональная количеству произошедших нарушений безопасности на предприятии за период в один год

60. Вредоносная, осуществляемая сознательно попытка человека или организации проникнуть в информационную систему другого человека или организации - это (возможно несколько вариантов):
    a. угроза
    b. уязвимость
    c. кибератака
    d. взлом

61. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ

к информации, определяемой по каким-либо признакам - это (возможно несколько вариантов):

a. пользователь информации
b. владелец информации
c. автор информации
d. носитель информации

62. От кого может получить информацию пользователь информации (выберите один вариант)?

a. собственника, владельца информации или посредника
b. только от посредника
c. только от собственника или владельца
d. только от автора информации

63. Конфиденциальность информации предполагает обязательное для выполнения лицом, получившим доступ к определенной информации… (выберите один вариант):

a. требование не вносить в такую информацию изменений и не создавать копии такую информации
b. требование не передавать такую информацию третьим лицам без согласия ее обладателя
c. требование не вносить в информацию изменений
d. требование не изменять, не копировать и не передавать такую информацию третьим лицам без согласия ее обладателя

64. Выберите программные средства защиты информации:

a. симметричное шифрование
b. файрволл
c. система видеонаблюдения
d. антивирус
e. электронный ключ-флешка

65. Программный или аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика - это:

a. антивирус
b. троянская программа
c. сетевой экран
d. комплексная система защиты информации

66. Рассылка по электронной почте мошеннических или вредоносных сообщений, которые выглядят так, будто они отправлены надежным адресатом - это (выберите один вариант):

a. фишинг
b. атака через посредника

c. внедрение вредоносного кода
d. DDoS-атака

67. В чем разница симметричного и асимметричного шифрования информации?
    a. асимметричное шифрование использует один ключ, симметричное - два разных: открытый для шифрования, закрытый для расшифровывания
    b. симметричное шифрование использует один ключ, асимметричное - два разных: закрытый для шифрования, открытый для расшифровывания
    c. асимметричное шифрование использует один ключ, симметричное - два разных: закрытый для шифрования, открытый для расшифровывания
    d. симметричное шифрование использует один ключ, асимметричное - два разных: открытый для шифрования, закрытый для расшифровывания

68. Информация, используемая криптографическим алгоритмом при шифровании / дешифровании сообщений, постановке и проверке цифровой подписи - это (выберите один вариант):
    a. код
    b. ключ
    c. карта
    d. пароль

69. Персональные данные это (выберите один вариант):
    a. любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу
    b. информация, прямо относящаяся к определенному или определяемому физическому лицу
    c. только так информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу, которая зафиксирована в федеральном законе “О персональных данных”
    d. любая информация, созданная физическим лицом или описывающая его

70. Биометрические персональные данные это (выберите один вариант):
    a. сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность
    b. только ограниченный набор физиологических и биологических особенностей: отпечатки пальцев и фотографическое изображение лица человека

c. любые сведения, которые характеризуют физиологические и биологические особенности человека
d. дактилоскопические данные, радужная оболочка глаз, анализы ДНК, на основании которых можно установить его личность

71. Выберите одно правильное утверждение:
a. кибербезопасность в энергетике важна, но угрозы кибербезопасности незначительны по сравнению с выгодами цифровой трансформации
b. кибербезопасность в энергетике является важнейшей проблемой цифровой трансформации
c. кибербезопасность в энергетике важна только для защиты данных от несанкционированного доступа
d. практически все проблемы кибербезопасность в энергетике решены за счет существующих правовой, аппаратной, программной и криптографических средств защиты

72. Для защиты объектов энергетики, которые используют цифровые технологии, нужно (возможно несколько вариантов ответа):
a. максимально разделять локальные вычислительные сети объектов энергетики и корпоративных сети предприятия, имеющие выход в Интернет
b. максимально интегрировать локальные вычислительные сети объектов энергетики и корпоративных сети предприятия, имеющие выход в Интернет
c. чтобы локальные вычислительные сети объектов энергетики имели защищенный собственный канал выхода в Интернет
d. разрабатывать и анализировать модели угроз, модели нарушителей и сценарии атак

73. Модель управления доступом к данным, не требующая назначения прав доступа к объектам данным каждому субъекту по-отдельности:
a. Ролевая модель
b. Матричная модель
c. Персонализированная модель
d. Объектная модель

74. Избирательное управление доступом предполагает использования кортежей:
a. объект-субъект-права
b. объект-субъект-роль
c. объект-субъект
d. субъект-права

75. Выберите все основные виды прав доступа к объектам данных:
    a. **чтение**
    b. **изменение (запись)**
    c. **администрование**
    d. удаление
    e. замена
    f. создание

76. «Банк данных угроз безопасности информации» ФСБ РФ содержит (выберите один вариант ответа):
    a. **базы данных по угрозам и уязвимостям**
    b. базу данных только угроз
    c. базу данных только уязвимостей
    d. только перечень нормативных документов в области защиты информации
    e. ничего из перечисленного

77. «Банк данных угроз безопасности информации» ФСБ РФ позволяет находить угрозы по (выберите все правильные варианты ответа):
    a. **контекстному поиску в названиях угроз**
    b. **источнику угрозы**
    c. **последствиям угрозы**
    d. степени влияния угрозы

78. «Банк данных угроз безопасности информации» ФСБ РФ позволяет находить уязвимости по (выберите все правильные варианты ответа):
    a. **контекстному поиску в названиях уязвимостей**
    b. **производителю программного обеспечения**
    c. **статусу уязвимости**
    d. наименованию связанной угрозы
    e. идентификатору угрозы по стандартам ISO

79. База знаний «Mitre ATT&CK» представляет собой (выберите один вариант ответа):
    a. **справочную систему с информацией о поведении злоумышленников, их тактиках и техниках**
    b. матрицу атак
    c. матрицу мер обеспечения кибербезопасности
    d. базу данных уязвимостей

80. База знаний «Mitre ATT&CK» представляет собой (выберите один вариант ответа):
    a. **справочную систему с информацией о поведении злоумышленников, их тактиках и техниках**

b. матрицу атак
c. матрицу мер обеспечения кибербезопасности
d. базу данных уязвимостей

81.Менеджмент риска (risk management) – это:

a. скоординированные действия по руководству и управлению организацией в области риска
b. система мер, направленных на снижение неопределенностей, связанных с рисками
c. скоординированные действия по минимизации последствий реализации рисков
d. система мер, направленных на выявление и устранение рисков организации

82.Риск – это:

a. это следствие влияния неопределенности на достижение поставленных целей
b. вероятность реализации события
c. вероятность недостижения поставленной цели из-за внешних воздействий на организацию
d. неопределенность достижения целей

83.Воздействие на риск – это:

a. процесс модификации риска
b. минимизация риска
c. оценка вероятности и последствий риска
d. снижение негативных последствий реализации риска

84.Установка резервных генераторов — это пример:

a. управления риском с помощью принятие мер по снижению возможных потерь
b. управления риском с помощью снижения уровня неопределенности
c. управления риском с помощью его разделения
d. управления риском с помощью страхования

85.Подход VaR в оценке рисков основан на учете:

a. правдоподобия и последствий события
b. последствий события и затрат на их устранение
c. затрат на минимизации последствий события и вероятности события
d. затрат на минимизации последствий события и правдоподобия события
e. последствий события и затрат на устранение возможности реализации события

86. Основной недостаток подхода VaR в оценке рисков:

a. невозможность достаточно точно определить вероятность события
b. невозможность достаточно точно опередить последствия события
c. невозможность достаточно точно опередить затраты на защиту от реализации события
d. невозможность получить количественную оценку риска

87. Фактор смягчения риска *RMF* можно определить как:

a. разность коэффициента α события до принятия мер и после принятия
b. отношение разности коэффициента α события до принятия мер и после принятия к его значению до принятия мер
c. отношение разности коэффициента α события до принятия мер и после принятия к затратам на реализацию мер
d. фактор смягчения риска определяется с помощью экспертной оценки от 0 до 1.

88. Если прямой ущерб от события составляет 100 млн. рублей, затраты на защиту – 15 млн. руб., а фактор смягчения риска *RMF* равен 0,2, то коэффициент возврата инвестиций в кибербезопасность равен

a. 0,33
b. 0,25
c. 0,75
d. 1,33

89. Если прямой ущерб от события составляет 15 млн. рублей, затраты на защиту – 5 млн. руб., а фактор смягчения риска *RMF* равен 0,4, то коэффициент возврата инвестиций в кибербезопасность равен

a. 0,2
b. 1,2
c. 0,33
d. -0,2

90. Если прямой ущерб от события составляет 8 млн. рублей, затраты на защиту – 4 млн. руб., а фактор смягчения риска *RMF* равен 0,1, то коэффициент возврата инвестиций в кибербезопасность равен

a. -0,8
b. 0,0
c. 0,2
d. -0,4

91. Критерий выбора стратегии защиты, который основан на учете наихудшего возможного варианта по каждой стратегии, называется:

a. макимин
b. минимакс
c. максимакс
d. минимин

92. Критерий выбора стратегии защиты, который основан на учете наилучшего возможного варианта по каждой стратегии, называется:

a. макимин
b. минимакс
c. максимакс
d. минимин

93. Укажите два главных требования к хэш-функции

a. знание значения хэш-функции не должно позволить восстановить исходные данные за приемлемое время
b. высокая скорость вычисления прямого и обратного значения хэш-функции
c. высокая вероятность получения разного результаты для различных входных данных
d. длина полученной хэш-суммы

94. Выберите из указанных алгоритмов хэширования два наиболее распространенных:

a. SHA256
b. MD5
c. SHA32
d. MD8

95. Укажите наиболее безопасный способ хранения паролей пользователей информационной системы

a. хранение паролей, закодированных с возможностью декодирования по ключу
b. хранение хэш-сумм паролей
c. хранение хэш-сумм, взятых от комбинации паролей и статической криптографической соли
d. хранение хэш-сумм, взятых от комбинации паролей и динамической криптографической соли

96. Для чего необходима криптографическая соль при хэшировании паролей?

a. Чтобы увеличить длину пароля

b. Чтобы злоумышленники не смогли узнать пароль по известному значению хэш-суммы, для которой известно входное значение
c. Чтобы администратор базы данных не имел доступа к паролям пользователей
d. Чтобы сократить объем памяти для хранения хэш-сумм паролей

97. Укажите, для каких задач обеспечения кибербезопасности может применять хэширование в цифровых подстанциях?
a. Аутентификация пользователей, входящих в информационную систему управления подстанцией
b. Обнаружение нештатной работы подстанции с помощью анализа значений тока и напряжения в узлах
c. Проверка сертификатов цифровых интеллектуальных устройств
d. Обнаружение подмены передаваемых сообщений

98. Выберите правильную последовательность действий при использовании электронной цифровой подписи.
a. вычисление хэш-суммы сообщения; шифрация хэш-суммы; добавление зашифрованной хэш-суммы к сообщению; отправка сообщения; вычисление хэш-суммы полученного сообщения без учета ЭЦП; расшифровка ЭПЦ; сравнение хэшей
b. вычисление хэш-суммы сообщения; добавление хэш-суммы к сообщению; отправка сообщения; вычисление хэш-суммы полученного сообщения без учета ЭЦП; сравнение хэшей
c. шифрация сообщения с помощью ключа ЭЦП; отправка сообщения; расшифровка полученного сообщения с помощью ключа ЭЦП.
d. вычисление хэш-суммы сообщения; шифрация хэш-суммы; добавление зашифрованной хэш-суммы к сообщению; отправка сообщения; вычисление хэш-суммы полученного сообщения; сравнение хэшей

99. Укажите три основных свойства данных, которые требуется защищать:
a. конфиденциальность, целостность, доступность
b. конфиденциальность, полнота, целостность
c. конфиденциальность, полнота, доступность
d. полнота, целостность, доступность

100. Внесение искажений в канал передачи данных нарушают (выберите один вариант):
a. целостность данных
b. конфиденциальность и целостность данных
c. доступность и целостность данных

d. доступность данных

4. Методические материалы, определяющие процедуры оценивания результатов освоения образовательной программы

Проведение оценки осуществляется путем сопоставления продемонстрированных обучающимся результатов освоения компетенций с заданными критериями.

Для положительного заключения по результатам оценочной процедуры по учебной дисциплине установлено пороговое значение показателя, при котором принимается положительное решение, констатирующее результаты освоения дисциплины.

4.1. Объекты оценивания и наименование оценочных средств

Формы текущего контроля успеваемости / формы промежуточной аттестации	Объекты оценивания	Вид занятия / наименование оценочных средств	Форма проведения оценки
Текущий контроль	Разделы дисциплины	Задания открытого типа и задания закрытого типа, относящиеся к разделу дисциплины	Электронная / письменная
Промежуточная аттестация	Обобщенные результаты обучения по дисциплине теоретических знаний и практических навыков	Задания открытого типа и задания закрытого типа из всех разделов дисциплины, сгруппированные в итоговый тест пропорционально трудоёмкости разделов	Электронная / письменная

4.2. Показатели, критерии и шкала оценки компетенций

Оценка знаний, умений, владений может быть выражена в параметрах «очень высокая», «высокая», соответствующая академической оценке «отлично» (в случае проведения по дисциплине экзамена или зачёта с оценкой) или «зачтено» (в случае проведения по дисциплине зачёта); «достаточно высокая», «выше средней», соответствующая академической оценке «хорошо» (в случае проведения по дисциплине экзамена или зачёта с оценкой) или «зачтено» (в случае проведения по дисциплине зачёта); «средняя», «ниже средней», «низкая», соответствующая академической оценке «удовлетворительно» (в случае проведения по дисциплине экзамена или зачёта с оценкой) или «зачтено» (в случае проведения по дисциплине зачёта); «очень низкая», соответствующая академической оценке «неудовлетворительно» (в случае проведения по дисциплине экзамена или зачёта с оценкой) или «не зачтено» (в случае проведения по дисциплине зачёта).

Текущий контроль и промежуточная аттестация

№ п/п	Виды работ	Критерии оценивания			
		Отсутствует компетенция	Базовый уровень освоения компетенции	Повышенный уровень освоения компетенции	Продвинутый уровень освоения компетенции
1.	Текущая аттестация: задания открытого типа и задания закрытого типа, относящиеся к разделу дисциплины	Выполнено менее 50% заданий	Выполнено от 50 до 60% заданий	Выполнено от 60 до 75% заданий	Выполнено свыше 75% заданий
2.	Выполнение диагностической работы (сформированной из банка оценочных материалов) при зачёте по итогам 2 семестра	Выполнено менее 50% заданий	Выполнено от 50 до 60% заданий	Выполнено от 60 до 75% заданий	Выполнено свыше 75% заданий

Критерии оценивания формулируются для каждой компетенции и отражают опознаваемую деятельность обучающегося, поддающуюся измерению.

Обобщенные критерии оценивания освоения компетенции

Не зачтено / не удовлетворительно	Зачтено / Удовлетворительно	Зачтено / Хорошо	Зачтено / Отлично
Отсутствует компетенция	**Базовый уровень освоения компетенции**	**Повышенный уровень освоения компетенции**	**Продвинутый уровень освоения компетенции**
Компетенция не освоена. Обучающийся частично показывает знания, входящие в состав компетенции, понимает их необходимость, но не может их применять.	Компетенция освоена. Обучающийся показывает общие знания, входящие в состав компетенции, имеет представление об их применении, умение извлекать и использовать основную (важную) информацию из полученных знаний	Компетенция освоена. Обучающийся показывает полноту знаний, демонстрирует умения и навыки решения типовых задач.	Компетенция освоена. Обучающийся показывает глубокие знания, демонстрирует умения и навыки решения сложных задач, умение принимать решения, создавать и применять документы, связанные с профессиональной деятельностью; способен самостоятельно решать проблему/задачу на основе изученных методов, приемов и технологий.

Базовый уровень освоения компетенций - обязательный для всех обучающихся по завершении освоения дисциплины.

Повышенный уровень освоения компетенций - превышение минимальных характеристик сформированности компетенции для обучающегося.

Продвинутый уровень освоения компетенций - максимально возможная выраженность компетенции, важен как качественный ориентир для самосовершенствования так и дополнительное к требованиям ОПОП освоение компетенций с учетом личностных характеристик:

- активное участие в конференциях, конкурсах, круглых столах и т.д. с получением зафиксированного положительного результата по вопросам, включенным в дисциплину;
- разработка и реализация проектов с применением компетенций, указанных в рабочей программе;
- демонстрирует умение применять теоретические знания для решения практических задач повышенной сложности и нестандартных задач;
- выполнение в срок всех поставленных задач.

Шкала критериев оценивания компетенций

Оценка	Содержание
Не зачтено / не удовлетворительно	Демонстрирует непонимание проблемы. Многие требования, предъявляемые к заданию не выполнены. Демонстрируется первичное восприятие материала. Работа незакончена и /или это плагиат.
Зачтено / удовлетворительно	Демонстрирует частичное понимание проблемы. Большинство требований, предъявляемых, к заданию выполнены. Владение элементами заданного материала. В основном выполненный материал понятен и носит целостный характер.
Зачтено / хорошо	Демонстрирует значительное понимание проблемы обозначенной дисциплиной. Все требования, предъявляемые к заданию выполнены. Содержание выполненных заданий раскрыто и рассмотрено с разных точек зрения.
Зачтено / отлично	Демонстрирует полное понимание проблемы. Все требования, предъявляемые к заданию выполнены. Продемонстрировано уверенное владение материалом дисциплины. Выполненные задания носят целостных характер, выполнены в полном объеме, структурированы, представлены различные точки зрения, продемонстрирован творческий подход.

Методические материалы, определяющие процедуры оценивания

Текущий контроль успеваемости осуществляется: на лекциях, практических (семинарских) и лабораторных занятиях.

Обучающиеся заранее информируются о критериях и процедуре текущего контроля успеваемости преподавателями по соответствующей учебной дисциплине (модуля). Успеваемость при текущем контроле характеризует объем и качество выполненной обучающимся работы по дисциплине (модулю).

Педагогические виды и формы, используемые в процессе текущего контроля успеваемости обучающихся, определяются преподавателем. Выбираемый вид текущего контроля обеспечивает наиболее полный и объективный контроль (измерение и фиксирование) уровня освоения результатов обучения по дисциплине.

В целях обеспечения текущего контроля успеваемости преподаватель проводит консультации.

Промежуточная аттестация обучающихся является формой контроля результатов обучения по дисциплине с целью комплексного определения соответствия уровня и качества знаний, умений и навыков обучающихся требованиям, установленным образовательной программой.

5. Особенности освоения дисциплины для инвалидов и лиц с ограниченными возможностями

Обучение обучающихся с ограниченными возможностями здоровья при необходимости осуществляется на основе адаптированной рабочей программы с использованием специальных методов обучения и дидактических материалов, составленных с учетом особенностей психофизического развития, индивидуальных возможностей и **при необходимости обеспечивающих коррекцию нарушений развития и социальную адаптацию указанных лиц**.

Самостоятельная работа обучающихся с ограниченными возможностями здоровья и инвалидов позволяет своевременно выявить затруднения и отставание и внести коррективы в учебную деятельность. Конкретные формы и виды самостоятельной работы обучающихся лиц с ограниченными возможностями здоровья и инвалидов устанавливаются преподавателем. Выбор форм и видов самостоятельной работы, обучающихся с ограниченными возможностями здоровья и инвалидов осуществляется с учетом их способностей, особенностей восприятия и готовности к освоению учебного материала. Формы самостоятельной работы устанавливаются с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге или на компьютере, в форме тестирования, электронных тренажеров и т.п.).

Основные формы представления оценочных средств – в печатной форме или в форме электронного документа. Для обучающихся с нарушениями зрения предусматривается возможность проведения текущего и промежуточного контроля в устной форме. Для обучающихся с нарушениями слуха предусматривается возможность проведения текущего и промежуточного контроля в письменной форме.

Категории обучающихся с ОВЗ, способы восприятия ими информации и методы их обучения

Категории обучающихся по нозологиям		**Методы обучения**
С нарушениям и зрения	Слепые. Способ восприятия информации: осязательно-слуховой.	*Аудиально-кинестетические*, предусматривающие поступление учебной информации посредством слуха и осязания. Могут использоваться при условии, что визуальная информация будет адаптирована для лиц с нарушениями зрения:
	Слабовидящие.	*визуально-кинестетические*, предполагающие передачу и восприятие

Категории обучающихся по нозологиям		Методы обучения
	Способ восприятия информации: зрительно-осязательно-слуховой	учебной информации при помощи зрения и осязания; *аудио-визуальные*, основанные на представление учебной информации, при которых задействовано зрительное и слуховое восприятие; *аудио-визуально-кинестетические*, базирующиеся на представлении информации, которая поступает по зрительному, слуховому и осязательному каналам восприятие.
С нарушениями слуха	Глухие. Способ восприятия информации: зрительно-осязательный.	*Визуально-кинестетические*, предполагающие передачу и восприятие учебной информации при помощи зрения и осязания. Могут использоваться при условии, что аудиальная информация будет адаптирована для лиц с нарушениями слуха: *аудио-визуальные*, основанные на представление учебной информации, при которых задействовано зрительное и слуховое восприятие; *аудиально-кинестетические*, предусматривающие поступление учебной информации посредством слуха и осязания; *аудио-визуально-кинестетические*, базирующиеся на представлении информации, которая поступает по зрительному, слуховому и осязательному каналам восприятие.
	Слабослышащие. Способ восприятия информации: зрительно-осязательно-слуховой	
С нарушениями опорно-двигательного аппарата	Способ восприятия информации: зрительно-осязательно-слуховой	− *визуально-кинестетические*; − *аудио-визуальные*; − *аудиально-кинестетические*; − *аудио-визуально-кинестетические*.

Способы адаптации образовательных ресурсов

Условные обозначения:

«+» – образовательный ресурс, не требующий адаптации;

«АФ» – адаптированный формат к особенностям приема-передачи информации обучающихся инвалидов и лиц с ОВЗ формат образовательного ресурса, в том числе с использованием специальных технических средств;

«АЭ» – альтернативный эквивалент используемого ресурса

Категории обучающихся по нозологиям		Образовательные ресурсы				
		Электронные				Печатные
		мультимедиа	графические	аудио	текстовые, электронные аналоги печатных изданий	
С нарушениями зрения	Слепые	АФ	АЭ (например, создание материальной модели графического объекта (3Dмодели)	+	АЭ (например, аудио описание)	АЭ (например, печатный материал, выполненный рельефно-точечным шрифтом Л.Брайля)
	Слабовидящие	АФ	АФ	+	АФ	АФ
С нарушениями слуха	Глухие	+	+	АЭ (например, Текстовое описание, гиперссылки)	+	+
	Слабослышащие	+	+	АФ	+	+
С нарушениями опорно-двигательного аппарата		+	+	+	+	+

Формы контроля и оценки результатов обучения инвалидов и лиц с ОВЗ

Категории обучающихся по нозологиям	Форма контроля и оценки результатов обучения
С нарушениями зрения	− устная проверка: дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.; − с использованием компьютера и специального ПО: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, дистанционные формы, если позволяет острота зрения - графические работы и др.
С нарушениями слуха	− письменная проверка: контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.; − с использованием компьютера и специального ПО: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы и др.
С нарушениями опорно-двигательного аппарата	− письменная проверка, с использованием специальных технических средств (альтернативных средства ввода, управления компьютером и др.): контрольные, графические работы, тестирование, домашние задания, эссе, письменные коллоквиумы, отчеты и др.; − устная проверка, с использованием специальных технических средств (средств коммуникаций): дискуссии, тренинги, круглые столы, собеседования, устные коллоквиумы и др.; − с использованием компьютера и специального ПО (альтернативных средств ввода и управления компьютером и др.): работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты, графические работы, дистанционные формы – предпочтительнее обучающимся, ограниченным в передвижении и др.

Задания для текущего контроля для инвалидов и лиц с ограниченными возможностями

Текущий контроль и промежуточная аттестация обучающихся инвалидов и лиц с ОВЗ осуществляется с использованием оценочных средств, адаптированных к ограничениям их здоровья и восприятия информации, в том числе с использованием специальных технических средств.

Текущий контроль успеваемости для обучающихся инвалидов и лиц с ОВЗ направлен на своевременное выявление затруднений и отставания в обучении и внесения коррективов в учебную деятельность. Возможно осуществление входного контроля для определения его способностей, особенностей восприятия и готовности к освоению учебного материала.

Задания для промежуточной аттестации для инвалидов и лиц с ограниченными возможностями

Форма промежуточной аттестации устанавливается с учетом индивидуальных психофизических особенностей (устно, письменно на бумаге, письменно на компьютере, в форме тестирования и т.п.). При необходимости обучающимся предоставляется дополнительное время для подготовки ответа.

Промежуточная аттестация, при необходимости, может проводиться в несколько этапов. Для этого рекомендуется использовать рубежный контроль, который является контрольной точкой по завершению изучения раздела или темы дисциплины, междисциплинарного курса, практик и ее разделов с целью оценивания уровня освоения программного материала. Формы и срок проведения рубежного контроля определяются преподавателем с учетом индивидуальных психофизических особенностей обучающихся.