Федеральное агентство по рыболовству
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Калининградский государственный технический университет»
(ФГБОУ ВО «КГТУ»)

УТВЕРЖДАЮ
Начальник УРОПСП

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат:
0174a99400e2af6fb74dca3b394e65efc4
Владелец: Мельникова Виктория Александровна
Действителен: с 12.04.2023 по 12.04.2024

Фонд оценочных средств
(приложение к рабочей программе дисциплины)

«ИНОСТРАННЫЙ ЯЗЫК»

основной профессиональной образовательной программы специалитета
по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

ИНСТИТУТ — Цифровых технологий
РАЗРАБОТЧИК — Кафедра иностранных языков

1 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Таблица 1 – Планируемые результаты обучения по дисциплине, соотнесенные с установленными индикаторами достижения компетенций

Код и наименование компетенции	Индикаторы достижения компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
УК-4: Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1: Демонстрирует умение вести обмен профессиональной информацией в устной и письменной формах, в том числе на иностранном(ых) языке(ах)	Иностранный язык	*Знать:* базовую лексику, представляющую стиль общетехнического общения, касающуюся тем, связанных с культурой, наукой, техникой, базовые грамматические правила, базовую лексику профессионального языка, наиболее употребительную грамматику и основные грамматические явления; частотный языковой материал профессионального общения и теоретические положения по темам, предусмотренным рабочей программой курса; базовую лексику профессионального языка, наиболее употребительную грамматику и основные грамматические явления; по темам, предусмотренным рабочей программой курса. *Уметь*: общаться в простых типичных ситуациях, требующих непосредственного обмена информацией в рамках тем, предусмотренных рабочей программой курса; поддерживать краткий разговор на профессиональные темы; писать простые сообщения и письма делового характера; находить конкретную информацию в простых общетехнических текстах. Понимать основные положения четко произнесенных высказываний в пределах литературной нормы на известные темы, связанные с профессиональными интересами; общаться в большинстве

Код и наименование компетенции	Индикаторы достижения компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
			ситуаций, возникающих в ходе профессионального общения; без предварительной подготовки участвовать в диалогах на знакомую / интересующую тему (например, «Information security»; «Computer in my life», “What is a virus?” “Internet Security”) владеть основными навыками письма для ведения переписки по общетехническим и общекультурным темам. Понимать устную (монологическую и диалогическую) речь на общетехнические темы, владеть наиболее употребительной грамматикой и основными грамматическими явлениями, характерными для устной и письменной речи профессиональной коммуникации. *Владеть:* синтаксическими структурами с заученными конструкциями, словосочетаниями и стандартными оборотами для того, чтобы передавать информацию в ситуациях делового общения; некоторыми навыками письменного перевода специализированной литературы (по специальности обучения), дающими возможность правильно понять общий смысл текста, а также основными навыками применения грамматических конструкций, изучаемых в соответствии с рабочей программой. Основными навыками устной и письменной речи в рамках, предусмотренных рабочей программой курса, основными навыками письменного перевода специализированной литературы (по специальности обучения), а также основными навыками

Код и наименование компетенции	Индикаторы достижения компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями/индикаторами достижения компетенции
			применения грамматических конструкций, изучаемых в соответствии с рабочей программой. При этом допускаются незначительные ошибки или недочеты, не меняющие смысл высказывания и не влияющие на успешность коммуникации. Высоким уровнем контроля грамматической правильности; уверенно владеть навыками устного и письменного перевода специализированной литературы (по специальности обучения), навыками применения сложных грамматических конструкций, изучаемых в соответствии с рабочей программой; приемами самостоятельной работы с языковым материалом (лексикой, грамматикой, фонетикой) с использованием справочной и учебной литературы.

2 ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПОЭТАПНОГО ФОРМИРОВАНИЯ РЕЗУЛЬТАТОВ ОСВОЕНИЯ ДИСЦИПЛИНЫ (ТЕКУЩИЙ КОНТРОЛЬ) И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

2.1 Для оценки результатов освоения дисциплины используются:

- оценочные средства текущего контроля успеваемости;

- оценочные средства для промежуточной аттестации по дисциплине.

2.2 К оценочным средствам текущего контроля успеваемости относятся:

- тестовые задания;

- задания по темам практических занятий.

2.3 К оценочным средствам для промежуточной аттестации по дисциплине, проводимой в форме зачета/экзамена, относятся:

- экзаменационные вопросы и(или) задания.

Промежуточная аттестация в форме зачета проходит по результатам прохождения всех видов текущего контроля успеваемости.

3 ОЦЕНОЧНЫЕ СРЕДСТВА ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ

3.1 Тестовые задания используются для оценки освоения всех тем дисциплины студентами. Тесты сформированы на основе материалов и вопросов рассмотренных в рамках практических занятий. Тесты являются наиболее эффективной и объективной формой оценивания знаний, умений и навыков, позволяющей выявлять не только уровень учебных достижений, но и структуру знаний, степень ее отклонения от нормы по профилю ответов учащихся на тестовые задания.

Тестирование обучающихся проводится в электронной среде вуза (в течении 10-15 минут, в зависимости от уровня сложности материала) после рассмотрения на лекциях соответствующих тем. Тестирование проводится с помощью компьютерной программы Indigo с возможность сетевого доступа. Типовые задания для тестирования представлены в приложении № 1.

Положительная оценка («отлично», «хорошо» или «удовлетворительно») выставляется программой автоматически, в зависимости от количества правильных ответов.

Градация оценок:

- «отлично» - свыше 85 %
- «хорошо» - более 70%, но не выше 85%
- «удовлетворительно» - свыше 55%, но не более 70%

3.2 В приложении № 2 приведены типовые задания по темам практических занятий и вопросы, рассматриваемые на них. Задания для подготовки к практическим занятиям и материал необходимый для подготовки к ним, в том числе показатели, критерии и шкалы оценивания результатов, представлены в учебно-методическом пособии, размещенном в электронной среде.

Ниже приведена универсальная система оценивания лексико-грамматических тестов/работ (таблица 2), минимальные показатели качества речевых умений(нормативы) и рекомендуемый минимальный объём и режим учебной деятельности студента в каждом семестре (таблицы 3, 4, 5, 6).

Таблица 2 - Оценка лексико-грамматических тестов и лексико-грамматических работ по иностранным языкам

Уровни	Оценка	Лексико-грамматические контрольные тесты, работы
Не зачтено Неудовлетворительно	0	Отсутствие работы, отказ от работы или допущение 30 и более грамматических, 30 и более лексических ошибок на изученный материал
	2	25-29 грамматических, 25-29 лексических ошибок на изученный материал.

		20-24 грамматических, 20-24 лексических ошибок на изученный материал.
Удовлетворительно	3	15-19 грамматических, 15-19 лексических ошибок на изученный материал.
		10-14 грамматических, 10-14 лексических ошибок на изученный материал.
Хорошо	4	7-9 грамматических, 7-9 лексических ошибок на изученный материал.
		4-5 грамматических, 4-5 лексических ошибок на изученный материал.
		2-3 грамматических, 4-5 лексических ошибок на изученный материал.
Отлично	5	1 грамматическая, 2-3 лексических ошибок на изученный материал.
		Отсутствие ошибок на изученный материал

Таблица 3 - Устная речь

Семест-ры	Минимальные показатели качества речевых умений (нормативы) на конец семестра	Рекомендуемый минимальный объём и режим учебной деятельности студента в каждом семестре
1	2	3
I семестр	а/ Умение высказаться в монологической форме по одной из тем, пройденных в течение семестра, участвовать в беседе по данной и смежным темам. Минимальный объем высказывания – **15-20** предложений. Высказывание должно убедительно и полно раскрывать тему. В процессе речи студент должен продемонстрировать достаточный словарный запас тематической и общей лексики, а также владение грамматикой соответствующего языка, достаточное для успешного общения на данном языке.	Рекомендуемое минимальное количество подготовленных лично, предъявленных преподавателю и проверенных им распространенных монологических высказываний в течение семестра – **8 - 10.** Тематика речи: повседневная, общественно-политическая, страноведческая – в соответствии с содержанием запланированных для изучения в первом семестре уроков базового учебника по курсу иностранного языка.
	б/ Умение расспросить собеседника о чем-либо в соответствии с целевым заданием: способность без подготовки сформулировать **5-7** вопросов, согласно поставленной задаче.	В течение семестра студенту рекомендуется регулярно (желательно - на каждом занятии) предъявлять на контроль преподавателю самостоятельно сформулированные вопросы на иностранном языке, незамедлительно выясняя и устраняя причины сделанных ошибок. Для достижения более активной практики в постановке вопросов, вопросы на иностранном языке рекомендуется формулировать письменно (в ходе домашней самоподготовки) и устно (на занятиях).

II семестр	а/ Монологическое высказывание по комплексной теме, обобщающей несколько пройденных тем, собственный анализ изученных в курсе иностранного языка проблем, формулирование собственного мнения в связи с изученной тематикой и обсуждавшимися в течение семестра проблемами. Речь студента должна показывать владение изученными сложными грамматическими формами и структурами иностранного языка, а также достаточным тематическим и общим словарным запасом. Минимальный объем высказывания – **15-20** предложений.	Рекомендуемое минимальное количество лично подготовленных распространенных монологических высказываний в течение семестра - **8-10**. Тематика речи: повседневная, научно-популярная, страноведческая, общественно-политическая – в соответствии с пройденными темами учебника.
	б/ Участие в беседе на заданную тему с опорой на целевое задание или ситуацию: студент должен уметь понятно и аргументировано высказаться на иностранном языке по любой из пройденных в течение семестра тем или ситуаций в объеме **5-7** реплик, демонстрируя достаточный словарный запас и владение наиболее типичными грамматическими структурами устной речи.	В течение семестра каждому студенту рекомендуется подготовить совместно с товарищами по группе и предъявить на контроль преподавателю не менее **4-5** развернутых диалогов, а также активно участвовать в устном общении на иностранном языке в ходе занятий.
III семестр	а/ Умение выступить с индивидуально подготовленным докладом (презентацией, сообщением) на иностранном языке на заранее выбранную тему. Выступление готовится на основе прочитанного в течение семестра объемного текстового материала. Время выступления – до **5-7** минут. Выступление должно быть понятным, грамотным и логичным. Оно должно достаточно полно раскрывать заявленную тему и соответствовать нормам иноязычной публичной речи.	В течение семестра каждый студент имеет возможность получить **2-4** консультации преподавателя по подготовке доклада. Студенту предоставляется возможность выступить с подготовленным докладом перед группой (потоком, на студенческой конференции кафедры), получив адекватную оценку и индивидуальные рекомендации на будущее.

	б/ Умение высказаться на иностранном языке по одной из пройденных в течение семестра комплексных тем.	Рекомендуемое количество индивидуально подготовленных распространенных монологических высказываний в течение семестра - 1**0-12.** Тематика речи: общественно-политическая, страноведческая, деловая, по широкому профилю специальности – в соответствии с материалом, пройденным в течение семестра.
	в/ Умение участвовать в диалоге/беседе общепрофессиональной и деловой направленности с целью обсуждения и совместного решения поставленной задачи, проблемы. Минимальное количество реплик в каждой ситуации – **5-7.**	В течение семестра рекомендуется подготовить и предъявить на контроль преподавателю не менее **5-7** развернутых диалогов/полилогов, а также активно участвовать в общении на иностранном языке во время занятий.
IV семестр	а/ Умение самостоятельно подготовить и выступить с докладом (сообщением, презентацией) на заранее выбранную тему (как правило, соответствующую теме курсовой работы по специальности). В ходе выступления необходимо продемонстрировать владение нормами публичной речи на данном иностранном языке, а также достаточным словарным запасом и грамматическими навыками устной речи.	В течение семестра рекомендуется, как минимум, **1-2** раза выступить с самостоятельно подготовленной презентацией (докладом, сообщением) на иностранном языке.
	б/ Умение участвовать в дебатах, коллективном обсуждении поставленной проблемы или дискуссионной темы; умение высказывать аргументы за и против, дополнить, поддержать высказывание собеседника или вежливо ему возразить. Способность вырабатывать в результате обсуждения общую линию поведения. В процессе речи на иностранном языке требуется показать достаточное владение грамматикой устной речи и продемонстрировать словарный запас, позволяющий свободно выражать свое мнение.	В течение семестра рекомендуется принять участие не менее, чем в **5-6** дискуссиях на иностранном языке. Ход и результаты дискуссий необходимо подробно обсудить и проанализировать с преподавателем и товарищами по группе.

Таблица 4 - Понимание иностранной речи на слух (*аудирование)*

Семестры	Минимальные показатели качества речевых умений (нормативы) на конец семестра	Рекомендуемый минимальный объём и режим учебной деятельности студентов в каждом семестре
1	**2**	**3**
I семестр	Понимание на слух монологической и диалогической речи носителей изучаемого иностранного языка, звучащей в среднем темпе. Длительность звучания при контрольном прослушивании - **1-1,5** минуты, максимальное количество прослушиваний - 2 раза. Проверка степени понимания проводится в тестовой форме, количество заданий в тесте – не менее **7-10.** Критерий успешности – выполнение не менее 60% заданий, адекватное представление студентом не менее 60% всех фактов (ключевых элементов информации), упоминавшихся в прослушанном тексте.	В течение семестра – на занятиях и дома - рекомендуется регулярно прослушивать тексты на иностранном языке, фиксируя понятое в виде выписок. В домашних условиях прослушайте текст многократно - столько раз, сколько Вам требуется, чтобы понять его основное содержание. Записывайте только то, в чем Вы абсолютно уверены. Проверяйте логику смысла и написание слов. Обращайте особое внимание на предлоги в словосочетаниях. Убедившись, что Вы правильно поняли и записали ключевые словосочетания прослушанного текста, старайтесь использовать их в своей устной речи. Не используйте в своей речи и на письме того, в чем Вы не уверены.
II семестр	Понимание на слух монологической и диалогической речи носителей языка общего, страноведческого, научно-популярного содержания. Длительность звучания при контрольном прослушивании – **1,5-2** минуты, максимальное количество прослушиваний – **2** раза. Форма проверки понимания – письменный ответ на вопросы (не менее **5** вопросов) или краткое письменное изложение на иностранном языке. Критерий успешности – адекватное представление не менее 60 % фактов (ключевых элементов информации), упоминавшихся в прослушанном тексте за время, не превышающее 35-40 минут. Отдельными отметками оцениваются: понимание аудиотекста и качество письменной речи.	В течение семестра – на занятиях и дома - рекомендуется регулярно прослушивать тексты на иностранном языке, фиксируя понятое в виде выписок. В домашних условиях прослушайте текст многократно - столько раз, сколько Вам требуется, чтобы понять его основное содержание. Записывайте только то, в чем Вы абсолютно уверены. Проверяйте логику смысла и написание слов. Обращайте особое внимание на предлоги в словосочетаниях. Убедившись, что Вы правильно поняли и записали ключевые словосочетания прослушанного текста, старайтесь использовать их в своей устной и письменной речи. Не используйте в своей речи того, в чем Вы не уверены.

III семестр	Понимание монологической и диалогической речи носителей языка страноведческого и профессионального содержания длительностью звучания до **2-2,5** минут. Форма проверки – письменное изложение содержания на иностранном языке за 40 минут или менее. Критерий успешности – адекватное представление не менее половины фактов (ключевых элементов информации), упоминавшихся в тексте. Отдельными отметками оцениваются: понимание аудиотекста и качество письменной речи.	В течение семестра рекомендуется регулярно (не реже 2-3 раз в неделю) прослушивать и излагать письменно содержание аудиотекстов соответствующей длины. При любой возможности старайтесь проверить точность понимания. Используйте аудиотексты как источник новых слов и словосочетаний для обогащения Вашей речи на иностранном языке. Привлекая в свою речь новые слова и словосочетания из прослушанного текста, тщательно проверьте их смысл, звучание, написание. Используйте только то, в чем Вы совершенно уверены.
IV семестр	Понимание на слух речи носителей изучаемого иностранного языка длительностью звучания **2,5-3,5** минуты по широкому или узкому профилю специальности при одно-/двукратном прослушивании. Форма проверки – письменное изложение ключевых элементов прослушанной информации на иностранном языке, анализ и оценка , выражение собственного мнения. Критерий успешности – правильное представление не менее половины фактов (ключевых элементов информации), упоминавшихся в аудитивном тексте, а также адекватное, логичное собственное заключение, оценка прослушанного. Время подготовки при контрольном прослушивании – до **30** минут.	В течение семестра рекомендуется регулярно прослушивать в аудитории и дома (не реже 2-3 раз в неделю) аудитивные материалы соответствующего содержания и сложности длительностью звучания не менее **2,5-3,5** минуты. В течение семестра студенту рекомендуется написать и проанализировать с преподавателем не менее **5** собственных изложений.

Таблица 5 - Чтение

Семест-ры	Минимальные показатели качества речевых умений (нормативы)	Рекомендуемый минимальный объём и режим учебной деятельности студентов в каждом семестре
1	**2**	**3**
I семестр	Контрольное чтение в конце семестра с пониманием общего	Рекомендуемый объем чтения за семестр – **19-20** тыс. печ. знаков текста. При этом

	содержания прочитанного: **1000-1200** печ. зн. текста повседневной, научно-популярной, общественно-политической или страноведческой тематики за **15** мин.; выразительное чтение вслух и устный перевод отмеченного отрывка; ответы на вопросы преподавателя по содержанию прочитанного.	рекомендуется не менее 8-**10** раз выполнить в классе и предъявить преподавателю / группе для проверки нормативные задания по чтению, постепенно доведя время выполнения до **15** минут и менее.
II семестр	Контрольное чтение с полным извлечением информации: в конце семестра студент должен уметь прочесть текст общего, общественно-политического или страноведческого содержания объемом **1200-1500** п. зн. за **20-25** мин., подготовить пересказ текста на иностр. языке и быть готовым выполнить выборочный устный перевод на русский язык **2-3**-х предложений по выбору преподавателя.	Рекомендуемый объем чтения для каждого студента за семестр – **22-26** тыс. печ. зн. текста. При этом каждому студенту необходимо, как минимум, 8-**10** раз за семестр выполнить данные задания в контрольном режиме, ставя своей целью постепенно приблизиться к требуемым временным нормативам и постоянно улучшая качество пересказа и перевода.
III семестр	Контрольное чтение с полным извлечением информации текста общепрофессиональной/общественно-политической направленности объемом **1800-2000** п. зн. за **15-20** минут, выполнение теста на проверку глубины и точности его понимания; пересказ[x] текста на иностранном языке, беседа с преподавателем по содержанию прочитанного.	Рекомендуемый объем чтения за семестр – **10-15** тыс. печ. зн. текста общепрофессиональной/общественно-политической направленности с обсуждением содержания на занятиях в группе, а также не менее **20** тыс. печ. зн. индивидуального чтения (индивидуальная тематическая подборка текстов) с презентацией и обсуждением содержания прочитанного в группе. Индивидуальное чтение советуем готовить из расчета пяти порций текста по **4** тыс. п. зн. каждый или четырех порций текста – по **5** тыс. печ. знаков. В течение семестра навыки понимания специального текста тренируются и проверяются также с помощью демонстрационных версий Федерального экзамена профессионального образования (ФЭПО), с которым можно ознакомиться на сайте www.fepo.ru.
IV семестр	1/Чтение с полным извлечением информации и анализом. Одна из форм проверки - *стилистически отшлифованный и терминологически выверенный* контрольный письменный и устный перевод текста по специальности.	Полное извлечение информации из прочитанного текста достигается в процессе его устного/письменного перевода на родной язык. При этом следует строго соблюдать стилистические нормы русского языка и проверять каждое переведенное предложение логикой здравого смысла, а

		также на соответствие описываемой ситуации. В профессиональных ситуациях следует обращать особое внимание на точное и осмысленное употребление терминов и их соответствие обсуждаемому предмету и теме.
	2/ Ознакомительное чтение текста объемом (**2-3** тыс. печ. зн.), краткое *письменное резюме* (*аннотация*) на иностранном языке и устное обсуждение с преподавателем/товарищами по группе содержания текста и соответствующей профессиональной/научно-популярной/страноведческой, общественно-политической проблемы. Время подготовки - **45** минут.	Для каждой порции индивидуального текста в ходе домашней подготовки требуется выполнить пересказ и письменную аннотацию на иностранном языке объемом примерно в половину страницы.

Таблица 6 - Письмо

Семест-ры	Минимальные показатели качества речевых умений (нормативы)	Рекомендуемый минимальный объём и режим учебной деятельности студентов в каждом семестре
1	**2**	**3**
I семестр	1/ В первом семестре следует научиться правильно и быстро заполнять анкету личных данных на иностранном языке. 2/ писать на иностранном языке автобиографию объемом **1-1,5** страницы. 3/ писать частное письмо в соответствии с целевым заданием объёмом **0,5-1** страницы за **25-30** минут. 4/ писать на иностранном языке сочинение на заданную тему, используя изученный в ходе семестра материал. Скорость написания сочинения к концу семестра - из расчета **1** страница за **30-45** минут.	Рекомендуемое количество письменных работ, подготовленных каждым студентом в течение семестра - **8-10**: автобиография, частное письмо – не менее **4-5** писем за семестр; сочинение - по завершении каждой пройденной темы, не менее **4-5** в течение семестра.
II семестр	1/ Умение написать частное письмо, адресованное конкретному лицу, в соответствии с целевым заданием.	Минимальное рекомендуемое количество писем, подготовленных каждым студентом в течение семестра, - **6-8**. Тематика писем: описание, благодарность, приглашение, предложение, впечатления.

	2/ Сочинение на заданную тему на основе изученного материала из расчета **1** страница за **25-30** минут.	Минимальное рекомендуемое количество сочинений, написанных каждым студентом в течение семестра, - **4-6.** Количество сочинений, как правило, должно соответствовать количеству пройденных в течение семестра тем.
III семестр	1/ Умение подготовить детальный письменный отчет/ доклад /презентацию на заранее определенную комплексную тему по широкому профилю специальности, общественно-политической, страноведческой или научно-популярной тематике, включая описание графиков и тенденций.	В течение семестра каждый студент должен индивидуально подготовить и предъявить на контроль преподавателю частями и в окончательном полном виде, как минимум, один отчет (доклад/презентацию), основанный на результатах обильного чтения и реферирования литературы по заданной теме.
	2/ Умение самостоятельно подготовить письменную аннотацию/ резюме прочитанного текста по широкому или узкому профилю специальности из расчета **0,5** страницы на **4-6** тыс. печатных знаков прочитанного текста. Контрольное время написания аннотации / резюме – до **30** минут.	В течение семестра каждый студент должен самостоятельно подготовить и предъявить на контроль преподавателю не менее **4-6** письменных аннотаций / резюме.
	3/ Умение написать сочинение на заданную тему из расчета **1** страница за **20-25** минут.	Рекомендуется написать не менее **4-6** сочинений (в соответствии с количеством пройденных тем).
IV семестр	1/ Умение написать сочинение на заданную тему из расчета 1страница за **20-25** минут.	Рекомендуется написать не менее **4-6** сочинений (в соответствии с количеством пройденных тем).
	2/ Умение самостоятельно подготовить реферат, доклад (презентацию, отчет) на основе прочитанной профессиональной литературы.	В течение семестра каждый студент должен индивидуально подготовить и предъявить на контроль преподавателю частями и в окончательном полном виде, как минимум, один реферат и один отчет (доклад/презентацию) по результатам обильного чтения специальной литературы (ориентировочно **20-25** тыс. печ. знаков за семестр).
	3/ Умение составить письменную аннотацию / резюме любого прочитанного специального текста из расчета **0,5-1** страница на **4-6** тыч. печ. зн. исходного текста. Время написания аннотации – **20-25** минут.	Рекомендуется подготовить и обсудить с преподавателем не менее **4-6** индивидуально подготовленных аннотаций / резюме в течение семестра.

4 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

4.1 Промежуточная аттестация по дисциплине проводится в форме зачета или экзамена (в зависимости от семестра обучения).

Зачет выставляется по результатам прохождения всех видов текущего контроля успеваемости. Оценка «зачтено» выставляется студентам, получившим положительную оценку («зачтено») по результатам выполнения заданий по темам практических занятий и тестирования.

В случае, если обучающийся пропустил более 50% занятий и его знания и умения не соответствуют заявленным компетенциям, то после соответствующего объема консультаций проводится зачет. Зачет проводится в два этапа: зачетная письменная работа и устный зачет. Устный зачет может в случае необходимости проводиться в несколько приемов, по отдельным аспектам. В ходе зачета устанавливается соответствие уровня развития умений устной речи, понимания на слух, понимания при чтении и письме на иностранном языке целевому уровню согласно Европейской шкале владения данным языком, а также *оценивается в баллах владение каждым из указанных речевых умений.*

Критерии оценивания при проведении промежуточной аттестации (экзамена): экзаменационная оценка является экспертной и зависит от уровня освоения студентом тем дисциплины (наличия и сущности ошибок, допущенных студентом при ответе на экзаменационные вопросы). Ответы на вопросы экзамена оцениваются по четырех балльной шкале («отлично», «хорошо», «удовлетворительно» «неудовлетворительно»); используются критерии этих оценок, описанных в таблице 7.

Вопросы для подготовки к экзамену представлены в приложении № 3.

Универсальная система оценивания результатов обучения включает в себя системы оценок: 1) «отлично», «хорошо», «удовлетворительно», «неудовлетворительно»; 2) «зачтено», «не зачтено»; 3) 100 – балльную/процентную систему и правило перевода оценок в пятибалльную систему (таблица 7).

Таблица 7 - Система оценок и критерии выставления оценки

Система оценок / Критерий	**2**	**3**	**4**	**5**
	0-40 %	**41-60 %**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
1. Системность и полнота знаний в отношении	Обладает частичными и разрозненными знаниями,	Обладает минимальным набором знаний, необходимым для	Обладает набором знаний, достаточным для системного	Обладает полнотой знаний и системным взглядом на изучаемый объект

Система оценок / Критерий	**2**	**3**	**4**	**5**
	0-40 %	**41-60 %**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
изучаемых объектов	которые не может научно корректно связывать между собой (только некоторые из которых может связывать между собой)	системного взгляда на изучаемый объект	взгляда на изучаемый объект	
2. Работа с информацией	Не в состоянии находить необходимую информацию, либо в состоянии находить отдельные фрагменты информации в рамках поставленной задачи	Может найти необходимую информацию в рамках поставленной задачи	Может найти, интерпрети-ровать и систематизи-ровать необходимую информацию в рамках поставленной задачи	Может найти, систематизиро-вать необходимую информацию, а также выявить новые, дополнитель-ные источники информации в рамках поставленной задачи
3. Научное осмысление изучаемого явления, процесса, объекта	Не может делать научно корректных выводов из имеющихся у него сведений, в состоянии проанализировать только некоторые из имеющихся у него сведений	В состоянии осуществлять научно корректный анализ предоставлен-ной информации	В состоянии осуществлять систематиче-ский и научно корректный анализ предоставлен-ной информации, вовлекает в исследование новые релевантные задаче данные	В состоянии осуществлять систематиче-ский и научно-корректный анализ предоставлен-ной информации, вовлекает в исследование новые релевантные поставленной задаче данные, предлагает новые ракурсы поставленной задачи
4. Освоение стандартных алгоритмов решения профессиональных задач	В состоянии решать только фрагменты поставленной задачи в соответствии с заданным алгоритмом, не освоил предложенный алгоритм, допускает ошибки	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом	В состоянии решать поставленные задачи в соответствии с заданным алгоритмом, понимает основы предложенного алгоритма	Не только владеет алгоритмом и понимает его основы, но и предлагает новые решения в рамках поставленной задачи

5 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «Иностранный язык» представляет собой компонент основной профессиональной образовательной программы по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация «Безопасность открытых информационных систем»).

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры иностранных языков (протокол № 06 от 28.03.2022 г.)

Заведующая кафедрой  Г.П. Кофанова

Фонд оценочных средств рассмотрен и одобрен на заседании кафедры информационной безопасности 20.04.2022 г. (протокол № 7).

Заведующая кафедрой  Н.Я. Великите

Приложение № 1

ТЕСТОВЫЕ ЗАДАНИЯ

УК-4: Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия

Индикатор достижения компетенции УК-4.1: Демонстрирует умение вести обмен профессиональной информацией в устной и письменной формах, в том числе на иностранном(ых) языке(ах)

Английский язык

Вариант 1.

The best answer is:

1. _____ you like this DVD?
a) Are b) Have c) Do

2. We _____ live in a flat.
a) don't b) hasn't c) doesn't

3. _____ he play tennis?
a)Where b) Does c) Do

4. We don't have _____ butter.
a) a b) any c) got

5. _____ some money here.
a) There're b) There c) There's

6. Everybody _____ wear a seat belt in the car.
a) must b) can c) doesn't have to

7. They _____ to go to France for a year.
a) decide b) deciding c) decided

8. We _____ lunch when you telephoned.
a) had b) were having c) are having

9. I can't find my glasses. I _____ them at the office.
a) had to leave b) could leave c) must have left

10. I never _____ the radio.
a) listen b) am listening c) listen to

11. We don't have ____ time.
a) much b) a c) plenty

12.The phone's ringing: _____ answer it.
a) I'll b) I c) will

13. I can't _____ another language.
a) speaking b) speak c) to speak

14. Stephen _____ to visit his parents.
a) will b) going c) is going

15. They won't come, _____ they?
a) won't b) come c) will

16. Every royal palace has _____ secrets.
a) the b) its c) his

17. They are going _____ in America next month.
a) to be b) will be c) be

18. They _____ to go to France for a year.
a) decide b) deciding c) decided

19. Football _____ in most countries.
a) plays b) is played c) is playing

20. Would you like ____ to the cinema with me?
a) go b) to go c) going

21. Waiter: "_____"
Visitor: "I'll just take a small salad, please."
1. Have you seen the menu?
2. May I take your order, madam?
3. What do you want?
4. Are you ready with the order at last?

22. Lecturer: "The highest temperature recorded on Earth is 57 degrees C in Death Valley."
Student: "_____"
1. I didn't catch it!
2. Could you repeat that more slowly, please?
3. I'd be really grateful if you repeated that.
4. Say that again!

23. Student: "I am sorry, I am not quite ready to answer today."
Professor: "_____"
1. How awful!
2. You never are.
3. I think you still have some time to correct it.
4. Oh, dear, you seem so tired today, have you got any problems?

24. Student 1: "Have you heard? Roy's split up with Mary".
Student 2: "Unbelievable! What's up?"
Teacher: "_____"
1. You must be quiet at the lessons.
2. Stop talking! I've told you three times.

3. What's the news?
4. Any troubles with the exercise? Could you be a bit quieter?

25. Student: "_____"
Teacher: "Yes, it was rather good. But pay attention to the mistakes I've underlined.

1. Have you seen my composition?
2. Excuse me, have you had time to check my composition?
3. If you don't mind, I'd like to know whether you had time to have a look at my composition?
4. I hope you have already marked my composition.

26. Director: "Good morning, Mr. Smith! How are you?"
Employee: "_____"

1. Not so great.
2. Never been better, thanks, how are you, Mr. Grey?
3. How do you do?
4. Very well, thank you.

27. Interviewer: "_____"
Candidate: "I'm looking for a position in which I can utilize my experience".

1. What type of position are you looking for?
2. What would you like?
3. Why have you come here?
4. What can I do for you?

28. Interviewer: "_____"
Candidate: " There is no prospect of promotion and I would like something more challenging."

1. Why have you chosen our company?
2. Why do you want to leave your present job?
3. Do you expect much money?
4. Could you tell us about your experience of working abroad?

29. Personnel Director: "When can you begin?"
Applicant: "_____"

1. Firstly, I have to solve some problems at my previous work. Secondly, I need a rest at least for a week
2. As soon as you would like me to begin.
3. Well, I don't know… .
4. Are you hiring me?

30. Mother: "Dear, you look awful – what's been happening?
Daughter: "_____"

1. Everything is great! I have just returned from a wonderful journey!
2. Well, Ok… Kenny and I have been arguing…
3. You'd better stop asking me.

Вариант 2.

The best answer is:

1. We _____ live in a flat.
a) don't b) hasn't c) doesn't

2. There isn't ____ milk in the fridge.
a) any b) some c) many

3. _____ are you from?
a) What b) Who c) Where

4. Have you _____ a car?
a) any b) have c) got

5. We _____ got a garage.
a) haven't b) hasn't c) don't

6. He has _____ breakfast.
a) ate b) eaten c) eat

7. They _____ pay for the tickets.
a) haven't to b) don't have c) don't have to

8. I don't _____ getting up early.
a) not like b) want c) enjoy

9. He _____ know how to spell it.
a) doesn't b) hasn't c) don't

10. Look! The sun _____ down.
a) goes b) is going c) go

11. We _____ to go to work at six in the morning.
a) must b) would c) had

12. He _____ like his brother.
a) look b) doesn't look c) isn't look

13. He said that most problems _____ by teenagers.
a) cause b) were caused d) were causing

14. We arrived at the station, but the bus _____ earlier.
a) has left b) had leave c) had left

15. I will do badly in my work, _____ try harder.
a) if I'm not b) if I haven't c) if I don'

16. In England children _____ wear school uniform at all times when they are in school.
a) must b) may c) can

17. He is a very cruel man. You really _____ try to forget him.
a) can b) must c) have to

18. You _____ come and stay with us sometime. We'll be glad to see you. (Casual invitation)
a) could b) will be able to c) must

19. I _____ get the bus to go to work every day.
a) have to b) must c) can

20. You _____ smoke at a gas station. It is dangerous!
a) can't b. don't have to c) mustn't

21. Shop-assistant: "_____"
Customer: "No. What have you got in the way of brown cotton jackets, size 38?"
1. Can I help you?
2. Are you being served?
3. Are you looking for jackets?
4. I'm afraid you look too fat in this.

22. Friend: "I've passed my driving test at last!"
You: "_____"
1. That's terrible.
2. That's terrific.
3. Guess what.
4. Listen! I have just started driving courses.

23. Boyfriend: "_____"
Girlfriend (in a coffee bar): "Yes, I'd like some of that fruit cake."
1. What can I get you to drink?
2. Do you fancy something to eat?
3. Oh, no! I've forgotten my wallet!
4. Would you care for ham sandwiches and a milk shake?

24. Boyfriend: "_____"
Girlfriend: "Are you saying I'm fat?"
1. You look beautiful today!
2. What's happened to you?
3. I'm falling in love with you.
4. Do you know how many calories there are in a bar of chocolate?

25. Teacher : "Could you help me take these dictionaries back?
Student: "_____"
1. I'm not responsible for the dictionaries today!
2. Oh, with great pleasure!
3. Yes, Mrs Smith. Could you tell me where to take them?
4. I'm in a terrible hurry, I will do it next time.

26. Wife: "_____"
Husband: "Paris is so romantic. I can't believe we're here together at last.
1. Why don't you invite me for a cup of coffee?

2. I'm so bored with this journey…
3. What a lovely view! The river's beautiful, isn't it?
4. Give up smoking!

27. Father: "I think you need a coat. It's going to be cold tonight.
Teenager: "_____"

1. Dad - nobody wears coats any more! Bye!
2. I will certainly put it on, Mum, and a hat, and warm mittens.
3. Are you cold?
4. Don't shout at me! I am not deaf.

28. You: "I'm going to Edinburgh".
Fellow-traveller: "_____"

1. That's really great! Congratulations!
2. Are you? So am I as it happens.
3. Oh, don't do it. An awful place.
4. Have you? That's interesting!

29. Guest: "Do you mind if I smoke here?"
Hostess: "_____"

1. You'd better give up such a bad habit.
2. I'd rather you smoked at your place.
3. Go ahead! Don't be so shy!
4. No, not at all.

30. Guest: "_____"
Hostess: "Thank you for coming."

1. I really should be off now. Good-bye!
2. I wish I would stay a little longer.
3. I think it's about time we left. Thank you for the delicious meal.
4. I'm dreadfully sorry, but I've broken a plate.

Вариант 3.

1. She never _____ the teacher.
a) listens b) is listening c) listens to

2.____ he like his English studies?
a) Do b) Is c) Does

3.They ___ live in the center of the town.
a) haven't b) don't c) doesn't

4. ___ she study?
a) Where b) Do c) Does

5. There isn't ____ milk in the fridge.
a) any b) some c) many

6. He _____ to Brazil on business.
a) go b) goes c) went

7. _____ is very good exercise.
a) Swim b) To swim c) Swimming

8. Are you _____ for one or two weeks?
a) staying b) stayed c) stay

9. We _____ like to see the mountains.
a) would b) will c) are

10. Look! The sun _____ down.
a) goes b) is going c) go

11. When I told her about it, she _____.
a) just laughed b) has just laughed c) was just laughing

12. Why _____ to the party tomorrow?
a) doesn't they come b) aren't they coming c) won't they to come

13. I tried to persuade her, but she _____ listen.
a) hasn't b) didn't c) hadn't

14. You _____ go and see this film: it's fantastic!
a) must b) can c) may

15. Passengers _____ fasten their seat belts.
a) can b) may c) must

16. We _____ leave at eleven o'clock last night because the last bus went at 11:30.
a) had to b) must c) might

17. We have been staying at a hotel for the last two weeks, so we _____ cook our own meals.
a) mustn't b) can't c) haven't had to

18. You _____ tell the boss what happened. He would never forgive us.
a) mustn't b) can't c) don't have to

19. You _____ go to Ajanta, a new Indian restaurant downtown. It's the best restaurant I have ever been to.
a) have to b) will be able to c) must

20. Paul _____ get up early in the morning, while everyone in this house does.
a) can't b) mustn't c) doesn't have to

The line most appropriate to the situation is:

21. Receptionist: "Savoy Hotel, reception desk. Can I help you?"
Tourist: "_____"

1. Would you be so kind to reserve a room for me if you have time?

2. I can offer you a single room equipped with all modern conveniences.
3. I would like to make a reservation for a week.
4. I need a room in an hour or two.

22. Receptionist: "_____"
Tourist: "C-h-e-r-n-o-v".

1. I can't hear well, I am sorry. Can you repeat, please?
2. I am sorry, I didn't quite catch your name. Could you spell it, please?
3. What is your name?
4. Can I help you, Mr…..?

23. Guest: "_____"
Receptionist: "Both. And you will find all conveniences there."

1. Can I have a single room with a private bath, not on the top floor?
2. Well… And what conveniences does it have?
3. Is there a shower in the room?
4. Is there a bath or a shower in the room?

24. Visitor: "_____"
Clerk: "How would you like the money?"

1. Can you give me £300?
2. I am expecting some money from my bank in London.
3. Can I open a savings account?
4. I'd like to change these pounds, please.

25. Visitor: "Could you cash this traveller' s cheque, please?"
Clerk: "_____"

1. Would you like to know the current rate for dollars, sir?
2. It's all the same to me.
3. How would you like it?
4. Shall I change this note for you, sir?

26. Customs officer: "_____"
Tourist: " Sure. Here it is."

1. Good morning! May I see your passport?
2. Show me your passport!
3. Would you be so kind to give me your passport, if you don't mind?
4. Do you have any cigarettes or alcohol?

27. Tourist: "_____"
Clerk (at the booking office of the airport) "I'll just see what there is."

1. Does the coach leave for the airport at 7.45?
2. By the way, when am I supposed to check in?
3. I'd like to book a flight to Munich for Monday the tenth.
4. Where is the plane, I wonder?

28. Passenger: "_____"
Taxi driver: "Certainly, madam. Don't worry!

1. I would really appreciate if you didn't drive so fast if it is possible.
2. A turtle goes faster than you!
3. Don't go so fast!

4. Could you drive not so fast, please?

29. Teacher: "_____"
Student: "He phoned me yesterday, he had caught the flu".

1. What sort of mood is Simon today?
2. Does anybody know what has happened to Simon?
3. What do you think of Simon?
4. How do you get on with Simon?

30. Student: "Peter is not feeling very well. He won't be able to come to the lecture."
Professor: "_____"

1. Oh, dear! What's up with him?
2. Let me know if there's anything I can do.
3. I am sorry to hear that. I hope he soon feels better.

I know such sort of sicknesses…A nice way to avoid writing the test!

Приложение № 2

ТИПОВЫЕ ЗАДАНИЯ ПО ТЕМАМ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Тема 1: Иностранный язык в техническом вузе.

Задание: Диалог-расспрос по заданной теме. Монологическое высказывание. Сочинение на заданную тему.

Вопросы для обсуждения:

- роль иностранного языка в образовании студентов технического вуза;
- цель и задачи дисциплины;
- место дисциплины в структуре образовательной программы;
- планируемые результаты освоения дисциплины.

Тема 2: Семья, дом, семейные традиции, уклад жизни.

Задание: визуализация; прослушивание оригинальных текстов по теме; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Сочинение на заданную тему.

Вопросы для обсуждения:

- представить свою семью;
- вести диалоги о семье;
- вести дискуссию по прочитанному;
- планировать содержание последующего устного или письменного изложения по теме.

Тема 3: Досуг, увлечения, путешествия, режим жизни в будние и выходные дни.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Сочинение на заданную тему.

Вопросы для обсуждения:

- предпочтения в свободное время;
- описать распорядок дня в выходные дни;
- договориться о встрече в выходной день и посещении места досуга (кино, театр, концерт, музей и т.д.);
- вести диалоги по теме, дискуссию по прочитанному;
- планировать содержание последующего устного или письменного изложения по теме.

Тема 4: Образование. Высшее образование в России и за рубежом. Мой вуз – КГТУ.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Сочинение на заданную тему.

Вопросы для обсуждения:

- моя учеба (на каком факультете, на каком направлении, на какой ступени, на каком курсе/семестре);
- изучаемые предметы;
- описать по схеме систему высшего образования в России и в стране.

Тема 5: Погода, климат.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Сочинение на заданную тему.

Вопросы для обсуждения:

- описание времен года;
- описание погоды;
- особенности климата в Калининградской области;
- любимое время года.

Тема 6: Город, транспорт, как пройти.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Сочинение на заданную тему.

Вопросы для обсуждения:

- мой город Калининград (немного истории, город сегодня);
- спросить и объяснить, как пройти или проехать куда-либо;
- ответить и описать, где расположен тот или иной городской объект;
- назвать основные городские достопримечательности;
- дать краткую историческую информацию о Калининграде (год основания, о довоенном и послевоенном городе).

Тема 7: Путешествия.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Сочинение на заданную тему.

Вопросы для обсуждения:

- куда я путешествую особенно охотно, на каком транспорте, привести аргументы почему (опасно/безопасно, быстро, свобода передвижения и т.д.), - когда я путешествую особенно охотно (летом/зимой, почему);
- рассказать (устно/письменно, в виде презентации о путешествии мечты).

Тема 8: Здоровье. У врача. Здоровый образ жизни.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Сочинение на заданную тему.

Вопросы для обсуждения:

- назвать самые распространенные заболевания;
- вести диалог в больнице, с врачом;
- сказать, что беспокоит, описать симптомы болезни;
- сказать, что, по-вашему, есть здоровый образ жизни (отсутствие вредных привычек, занятие спортом, здоровое питание).

Тема 9: Еда, покупки, магазины, посещение ресторана.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Сочинение на заданную тему.

Вопросы для обсуждения:

- назвать основные продукты питания;
- рассказать, где совершаются ежедневные и еженедельные покупки (в супермаркете, на рынке, в небольших магазинчиках);
- аргументировать почему: удобнее, дешевле, быстрее, качественнее);
- уметь вести диалог в ресторане; заказать еду, расплатиться.

Тема 10: Достижения мировой науки и техники. Великие ученые.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Сочинение на заданную тему.

Вопросы для обсуждения:

- какие достижения науки и техники играют важную роль в вашей жизни (компьютер, мобильный телефон, и т.д.), аргументировать почему;
- уметь вести диалог с консультантом по продажам, запрашивать техническую информацию об аппарате, уметь дискутировать о преимуществах и недостатках гаджета, выражать собственное мнение.

Тема 11: Охрана окружающей среды. Экологические движения.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Сочинение на заданную тему.

Вопросы для обсуждения:

- назвать основные экологические проблемы в мире (загрязнение воздуха, воды, почвы, вымирание лесов, проблема утилизации мусора;
- наиболее актуальные экологические проблемы в Калининградской области, - устно, письменно, в форме презентации представить возможные пути решения экологических проблем на изучаемом языке.

Тема 12: СМИ в мире. Информационные технологии XX – XI века. Плюсы и минусы всеобщей информатизации общества.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Сочинение на заданную тему.

Вопросы для обсуждения:

- назвать известные средства массовой информации (газеты, телевидение, радио, Интернет), сказать об их основных преимуществах и недостатках.

Тема 13: История моей профессии.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Сочинение на заданную тему.

Вопросы для обсуждения:

- основные вехи в развитии;
- изучаемая профессия в России и за рубежом;
- история, современное состояние и перспективы.

Тема 14: Введение в специальность.

Задание: визуализация; прослушивание оригинальных текстов по теме; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Реферат на заданную тему.

Вопросы для обсуждения:

- актуальность моей профессии;
- востребованность на рынке;
- обеспеченность отрасли специалистами.

Тема 15: Основные виды деятельности в моей профессии.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Сочинение на заданную тему.

Вопросы для обсуждения:

- спектр специализаций в рамках профессии;
- основные обязанности и задачи специалистов отрасли;
- локальные и территориальные возможности работы специалистов.

Тема 16: Преимущества и недостатки профессии.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Реферат на заданную тему.

Вопросы для обсуждения:

- актуальный рейтинг профессии;
- финансовая составляющая работы в отрасли;
- временная составляющая работы в отрасли;
- социальная составляющая работы в отрасли;
- возможности профессионального роста.

Тема 17: Будущее моей профессии.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Реферат на заданную тему.

Вопросы для обсуждения:

- современное состояние отрасли;
- прогнозы актуальности и развития отрасли в перспективе;

- анализ востребованности специалистов в отрасли.

Тема 18: Инновационные технологии в моей профессии.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Реферат на заданную тему.

Вопросы для обсуждения:

- оценка современного состояния применения инновационных технологий в профессии;
- конкретизировать, какие инновационные технологии задействованы в отрасли;
- цифровые технологии в отрасли.

Тема 19: Деловые коммуникации.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Деловое письмо на заданную тему.

Вопросы для обсуждения:

- использование телефона;
- начало и завершение разговора по телефону;
- обмен информацией, назначение встреч, изменение договоренностей;
- деловая переписка;
- стиль делового письма;
- электронная почта;
- стиль электронного сообщения.

Тема 20: Устройство на работу.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание. Написание резюме, сопроводительного письма.

Вопросы для обсуждения:

- задачи и обязанности специалистов, работающих в отрасли.
- наиболее востребованные профессии.
- перечень документов, необходимых для приема на работу.
- правильное оформление заявления о приеме на работу;
- типы резюме;
- правила написания резюме при приеме на работу;
- собеседование при приеме на работу;

- правила речевого этикета при собеседовании;
- наиболее часто задаваемые вопросы при собеседовании.

Тема 21: Деловая поездка.

Задание: визуализация; прослушивание оригинальных текстов по теме и выполнение устных/письменных заданий; чтение. Диалог-расспрос по заданной теме. Монологическое высказывание.

Вопросы для обсуждения:

- прибытие в страну;
- таможенный и паспортный контроль;
- в аэропорту, на вокзале, расписание, городской транспорт;
- бронирование отеля.

Приложение № 3

ЭКЗАМЕНАЦИОННЫЕ ВОПРОСЫ ПО ДИСЦИПЛИНЕ

Билет 1

TASK 1. Read the text and summarise it using the topic-related vocabulary.

What is Information Security (InfoSec)?

Information security (sometimes referred to as InfoSec) covers the tools and processes that organizations use to protect information. This includes policy settings that prevent unauthorized people from accessing business or personal information. InfoSec is a growing and evolving field that covers a wide range of fields, from network and infrastructure security to testing and auditing.

Information security protects sensitive information from unauthorized activities, including inspection, modification, recording, and any disruption or destruction. The goal is to ensure the safety and privacy of critical data such as customer account details, financial data or intellectual property.

The consequences of security incidents include theft of private information, data tampering, and data deletion. Attacks can disrupt work processes and damage a company's reputation, and also have a tangible cost.

Organizations must allocate funds for security and ensure that they are ready to detect, respond to, and proactively prevent, attacks such as phishing, malware, viruses, malicious insiders, and ransomware.

What are the 3 Principles of Information Security?

The basic tenets of information security are confidentiality, integrity and availability. Every element of the information security program must be designed to implement one or more of these principles. Together they are called the CIA Triad.

Confidentiality

Confidentiality measures are designed to prevent unauthorized disclosure of information. The purpose of the confidentiality principle is to keep personal information private and to ensure that it is visible and accessible only to those individuals who own it or need it to perform their organizational functions.

Integrity

Consistency includes protection against unauthorized changes (additions, deletions, alterations, etc.) to data. The principle of integrity ensures that data is accurate and reliable and is not modified incorrectly, whether accidentally or maliciously.

Availability

Availability is the protection of a system's ability to make software systems and data fully available when a user needs it (or at a specified time). The purpose of availability is to make the technology infrastructure, the applications and the data available when they are needed for an organizational process or for an organization's customers.

TASK 2. Choose the correct answer.

1. What is a firewall in computer security?
   a. A type of virus
   b. A software program
   c. A hardware device
   d. A computer network security system

2. What is the main purpose of an antivirus program?
   a. To protect a computer from viruses and other malicious software
   b. To backup data on a computer
   c. To manage passwords

d. To monitor network traffic

3. What is a strong password?
   a. A password containing only numbers
   b. A password that is easily guessed
   c. A password containing letters, numbers, and symbols
   d. A password containing only uppercase letters

4. What is a phishing attack?
   a. An attack that targets vulnerabilities in a computer's hardware
   b. A type of malware
   c. An attempt to steal sensitive information by pretending to be a trustworthy source
   d. A type of cyberattack that targets software vulnerabilities

5. What is the purpose of encryption?
   a. To scramble data so it can only be read by the intended recipient
   b. To speed up data transfer
   c. To protect data during transit
   d. To make data more organized

6. What is two-factor authentication?
   a. A security measure that requires two forms of identification before accessing a system
   b. A type of encryption
   c. A backup procedure
   d. A password manager

7. What is the purpose of a disaster recovery plan?
   a. To minimize the impact of a security breach
   b. To ensure that an organization can respond to a disaster or other emergency that affects information systems – and minimize the effect on business operations.
   c. To manage passwords
   d. To monitor network traffic

8. What is the difference between confidentiality, integrity, and availability in information security?
   a. Confidentiality means keeping information private, integrity means making sure information is accurate and trustworthy, and availability means making sure information is accessible when needed.
   b. Confidentiality means making sure information is accessible when needed, integrity means keeping information private, and availability means making sure information is accurate and trustworthy.
   c. Confidentiality means making sure information is accurate and trustworthy, integrity means keeping information private, and availability means making sure information is accessible when needed.
   d. Confidentiality means making sure information is accessible when needed, integrity means making sure information is accurate and trustworthy, and availability means keeping information private.

9. What is a man-in-the-middle attack?

a. An attack where an attacker intercepts and potentially alters communication between two parties
b. An attack where an attacker gains unauthorized access to a system by exploiting software vulnerabilities
c. An attack where an attacker steals sensitive information by pretending to be a trustworthy source
d. An attack where an attacker gains access to a system by guessing a password

10. What is social engineering in the context of information security?
a. A technique used to trick individuals into revealing sensitive information b. A type of software program
c. A security measure that requires two forms of identification before accessing a system
d. A hardware device used to protect a network from unauthorized access

TASK 3. Speak about the challenges you can face dealing with Cloud Computing.

Билет 2

TASK 1. Read the text and summarise it using the topic-related vocabulary.

Information Security vs Cybersecurity

Information security differs from cybersecurity in both scope and purpose. The two terms are often used interchangeably, but more accurately, cybersecurity is a subcategory of information security. Information security is a broad field that covers many areas such as physical security, endpoint security, data encryption, and network security. It is also closely related to information assurance, which protects information from threats such as natural disasters and server failures.

Cybersecurity primarily addresses technology-related threats, with practices and tools that can prevent or mitigate them. Another related category is data security, which focuses on protecting an organization's data from accidental or malicious exposure to unauthorized parties.

Information Security Policy

An Information Security Policy (ISP) is a set of rules that guide individuals when using IT assets. Companies can create information security policies to ensure that employees and other users follow security protocols and procedures. Security policies are intended to ensure that only authorized users can access sensitive systems and information.

Creating an effective security policy and taking steps to ensure compliance is an important step towards preventing and mitigating security threats. To make your policy truly effective, update it frequently based on company changes, new threats, conclusions drawn from previous breaches, and changes to security systems and tools.

Make your information security strategy practical and reasonable. To meet the needs and urgency of different departments within the organization, it is necessary to deploy a system of exceptions, with an approval process, enabling departments or individuals to deviate from the rules in specific circumstances.

Top Information Security Threats

There are hundreds of categories of information security threats and millions of known threat vectors. Below we cover some of the key threats that are a priority for security teams at modern enterprises.

Unsecure or Poorly Secured Systems

The speed and technological development often leads to compromises in security measures. In other cases, systems are developed without security in mind, and remain in operation at an organization as legacy systems. Organizations must identify these poorly secured systems, and mitigate the threat by securing or patching them, decommissioning them, or isolating them.

TASK 2. Choose the correct answer

1. What is a firewall in computer security?
   a. A type of virus
   b. A software program
   c. A hardware device
   d. A computer network security system

2. What is the main purpose of an antivirus program?
   a. To protect a computer from viruses and other malicious software
   b. To backup data on a computer
   c. To manage passwords
   d. To monitor network traffic

3. What is a strong password?
   a. A password containing only numbers
   b. A password that is easily guessed
   c. A password containing letters, numbers, and symbols
   d. A password containing only uppercase letters

4. What is a phishing attack?
   a. An attack that targets vulnerabilities in a computer's hardware
   b. A type of malware
   c. An attempt to steal sensitive information by pretending to be a trustworthy source
   d. A type of cyberattack that targets software vulnerabilities

5. What is the purpose of encryption?
   a. To scramble data so it can only be read by the intended recipient
   b. To speed up data transfer
   c. To protect data during transit
   d. To make data more organized

6. What is two-factor authentication?
   a. A security measure that requires two forms of identification before accessing a system
   b. A type of encryption
   c. A backup procedure
   d. A password manager

7. What is the purpose of a disaster recovery plan?
   a. To minimize the impact of a security breach
   b. To ensure that an organization can respond to a disaster or other emergency that affects information systems – and minimize the effect on business operations.
   c. To manage passwords
   d. To monitor network traffic

8. What is the difference between confidentiality, integrity, and availability in information security?
   a. Confidentiality means keeping information private, integrity means making sure information is accurate and trustworthy, and availability means making sure information is accessible when needed.

b. Confidentiality means making sure information is accessible when needed, integrity means keeping information private, and availability means making sure information is accurate and trustworthy.
c. Confidentiality means making sure information is accurate and trustworthy, integrity means keeping information private, and availability means making sure information is accessible when needed.
d. Confidentiality means making sure information is accessible when needed, integrity means making sure information is accurate and trustworthy, and availability means keeping information private.

9. What is a man-in-the-middle attack?
   a. An attack where an attacker intercepts and potentially alters communication between two parties
   b. An attack where an attacker gains unauthorized access to a system by exploiting software vulnerabilities
   c. An attack where an attacker steals sensitive information by pretending to be a trustworthy source
   d. An attack where an attacker gains access to a system by guessing a password

10. What is social engineering in the context of information security?
    a. A technique used to trick individuals into revealing sensitive information
    b. A type of software program
    c. A security measure that requires two forms of identification before accessing a system
    d. A hardware device used to protect a network from unauthorized access

TASK 3. Speak about databases. What kind of records and files do computer bases usually contain? Which databases would you choose for such vocational spheres as: distant learning; medicine; commerce; law; hospitality business; records keeping; school teaching; university education? Explain why.

Билет 3

TASK 1. Read the text and summarise it using the topic-related vocabulary.

Social Media Attacks

Many people have social media accounts, where they often unintentionally share a lot of information about themselves. Attackers can launch attacks directly via social media, for example by spreading malware via social media messages, or indirectly, by using information obtained from these sites to analyze user and organizational vulnerabilities, and use them to design an attack.

Social Engineering

Social engineering involves attackers sending emails and messages that trick users into performing actions that may compromise their security or divulge private information. Attackers manipulate users using psychological triggers like curiosity, urgency or fear.

Because the source of a social engineering message appears to be trusted, people are more likely to comply, for example by clicking a link that installs malware on their device, or by providing personal information, credentials, or financial details.

Organizations can mitigate social engineering by making users aware of its dangers and training them to identify and avoid suspected social engineering messages. In addition, technological systems can be used to block social engineering at its source, or prevent users from performing dangerous actions such as clicking on unknown links or downloading unknown attachments.

Malware on Endpoints

Organizational users work with a large variety of endpoint devices, including desktop computers, laptops, tablets, and mobile phones, many of which are privately owned and not under the organization's control, and all of which connect regularly to the Internet.

A primary threat on all these endpoints is malware, which can be transmitted by a variety of means, can result in compromise of the endpoint itself, and can also lead to privilege escalation to other organizational systems.

Traditional antivirus software is insufficient to block all modern forms of malware, and more advanced approaches are developing to securing endpoints, such as endpoint detection and response (EDR).

Lack of Encryption

Encryption processes encode data so that it can only be decoded by users with secret keys. It is very effective in preventing data loss or corruption in case of equipment loss or theft, or in case organizational systems are compromised by attackers.

Unfortunately, this measure is often overlooked due to its complexity and lack of legal obligations associated with proper implementation. Organizations are increasingly adopting encryption, by purchasing storage devices or using cloud services that support encryption, or using dedicated security tools.

TASK 2. Choose the correct answer.

1. What is a firewall in computer security?
   a. A type of virus
   b. A software program
   c. A hardware device
   d. A computer network security system

2. What is the main purpose of an antivirus program?
   a. To protect a computer from viruses and other malicious software
   b. To backup data on a computer
   c. To manage passwords
   d. To monitor network traffic

3. What is a strong password?
   a. A password containing only numbers
   b. A password that is easily guessed
   c. A password containing letters, numbers, and symbols
   d. A password containing only uppercase letters

4. What is a phishing attack?
   a. An attack that targets vulnerabilities in a computer's hardware
   b. A type of malware
   c. An attempt to steal sensitive information by pretending to be a trustworthy source
   d. A type of cyberattack that targets software vulnerabilities

5. What is the purpose of encryption?
   a. To scramble data so it can only be read by the intended recipient
   b. To speed up data transfer
   c. To protect data during transit
   d. To make data more organized

6. What is two-factor authentication?

a. A security measure that requires two forms of identification before accessing a system
b. A type of encryption
c. A backup procedure
d. A password manager

7. What is the purpose of a disaster recovery plan?
   a. To minimize the impact of a security breach
   b. To ensure that an organization can respond to a disaster or other emergency that affects information systems – and minimize the effect on business operations.
   c. To manage passwords
   d. To monitor network traffic

8. What is the difference between confidentiality, integrity, and availability in information security?
   a. Confidentiality means keeping information private, integrity means making sure information is accurate and trustworthy, and availability means making sure information is accessible when needed.
   b. Confidentiality means making sure information is accessible when needed, integrity means keeping information private, and availability means making sure information is accurate and trustworthy.
   c. Confidentiality means making sure information is accurate and trustworthy, integrity means keeping information private, and availability means making sure information is accessible when needed.
   d. Confidentiality means making sure information is accessible when needed, integrity means making sure information is accurate and trustworthy, and availability means keeping information private.

9. What is a man-in-the-middle attack?
   a. An attack where an attacker intercepts and potentially alters communication between two parties
   b. An attack where an attacker gains unauthorized access to a system by exploiting software vulnerabilities
   c. An attack where an attacker steals sensitive information by pretending to be a trustworthy source
   d. An attack where an attacker gains access to a system by guessing a password

10. What is social engineering in the context of information security?
    a. A technique used to trick individuals into revealing sensitive information
    b. A type of software program
    c. A security measure that requires two forms of identification before accessing a system
    d. A hardware device used to protect a network from unauthorized access

TASK 3. Speak about the phenomenon of Big Data and its application in different spheres of human activities.

Билет 4

TASK 1. Read the text and summarise it using the topic-related vocabulary.

Security Misconfiguration

Modern organizations use a huge number of technological platforms and tools, in particular web applications, databases, and Software as a Service (SaaS) applications, or Infrastructure as a Service (IaaS) from providers like Amazon Web Services.

Enterprise grade platforms and cloud services have security features, but these must be configured by the organization. Security misconfiguration due to negligence or human error can result in a security breach. Another problem is "configuration drift", where correct security configuration can quickly become out of date and make a system vulnerable, unbeknownst to IT or security staff.

Organizations can mitigate security misconfiguration using technological platforms that continuously monitor systems, identify configuration gaps, and alert or even automatically remediate configuration issues that make systems vulnerable.

Active vs Passive Attacks

Information security is intended to protect organizations against malicious attacks. There are two primary types of attacks: active and passive. Active attacks are considered more difficult to prevent, and the focus is on detecting, mitigating and recovering from them. Passive attacks are easier to prevent with strong security measures.

Active Attack

An active attack involves intercepting a communication or message and altering it for malicious effect. There are three common variants of an active attacks:

- **Interruption**—the attacker interrupts the original communication and creates new, malicious messages, pretending to be one of the communicating parties.
- **Modification**—the attacker uses existing communications, and either replays them to fool one of the communicating parties, or modifies them to gain an advantage.
- **Fabrication**—creates fake, or synthetic, communications, typically with the aim of achieving denial of service (DoS). This prevents users from accessing systems or performing normal operations.

Passive Attack

In a passive attack, an attacker monitors, monitors a system and illicitly copies information without altering it. They then use this information to disrupt networks or compromise target systems.

The attackers do not make any change to the communication or the target systems. This makes it more difficult to detect. However, encryption can help prevent passive attacks because it obfuscates the data, making it more difficult for attackers to make use of it.

TASK 2. Choose the correct answer.

1. What is a firewall in computer security?
   a. A type of virus
   b. A software program
   c. A hardware device
   d. A computer network security system

2. What is the main purpose of an antivirus program?
   a. To protect a computer from viruses and other malicious software
   b. To backup data on a computer
   c. To manage passwords
   d. To monitor network traffic

3. What is a strong password?
   a. A password containing only numbers
   b. A password that is easily guessed

c. A password containing letters, numbers, and symbols
d. A password containing only uppercase letters

4. What is a phishing attack?
   a. An attack that targets vulnerabilities in a computer's hardware
   b. A type of malware
   c. An attempt to steal sensitive information by pretending to be a trustworthy source
   d. A type of cyberattack that targets software vulnerabilities

5. What is the purpose of encryption?
   a. To scramble data so it can only be read by the intended recipient
   b. To speed up data transfer
   c. To protect data during transit
   d. To make data more organized

6. What is two-factor authentication?
   a. A security measure that requires two forms of identification before accessing a system
   b. A type of encryption
   c. A backup procedure
   d. A password manager

7. What is the purpose of a disaster recovery plan?
   a. To minimize the impact of a security breach
   b. To ensure that an organization can respond to a disaster or other emergency that affects information systems – and minimize the effect on business operations.
   c. To manage passwords
   d. To monitor network traffic

8. What is the difference between confidentiality, integrity, and availability in information security?
   a. Confidentiality means keeping information private, integrity means making sure information is accurate and trustworthy, and availability means making sure information is accessible when needed.
   b. Confidentiality means making sure information is accessible when needed, integrity means keeping information private, and availability means making sure information is accurate and trustworthy.
   c. Confidentiality means making sure information is accurate and trustworthy, integrity means keeping information private, and availability means making sure information is accessible when needed.
   d. Confidentiality means making sure information is accessible when needed, integrity means making sure information is accurate and trustworthy, and availability means keeping information private.

9. What is a man-in-the-middle attack?
   a. An attack where an attacker intercepts and potentially alters communication between two parties
   b. An attack where an attacker gains unauthorized access to a system by exploiting software vulnerabilities
   c. An attack where an attacker steals sensitive information by pretending to be a trustworthy source

d. An attack where an attacker gains access to a system by guessing a password

10. What is social engineering in the context of information security?
    a. A technique used to trick individuals into revealing sensitive information
    b. A type of software program
    c. A security measure that requires two forms of identification before accessing a system
    d. A hardware device used to protect a network from unauthorized access

TASK 3. Elaborate on the necessity of Big Data security. Speak about the new types of risks going along with using Big Data.

Билет 5

TASK 1. Read the text and summarise it using the topic-related vocabulary.

Information security, sometimes shortened to **InfoSec**, is the practice of protecting information by mitigating information risks. It is part of information risk management. It typically involves preventing or reducing the probability of unauthorized/inappropriate access to data, or the unlawful use, disclosure, disruption, deletion, corruption, modification, inspection, recording, or devaluation of information. It also involves actions intended to reduce the adverse impacts of such incidents. Protected information may take any form, e.g. electronic or physical, tangible (e.g. paperwork) or intangible (e.g. knowledge). Information security's primary focus is the balanced protection of the confidentiality, integrity, and availability of data (also known as the CIA triad) while maintaining a focus on efficient policy implementation, all without hampering organization productivity. This is largely achieved through a structured risk management process that involves:

- identifying information and related assets, plus potential threats, vulnerabilities, and impacts;
- evaluating the risks
- deciding how to address or treat the risks i.e. to avoid, mitigate, share or accept them
- where risk mitigation is required, selecting or designing appropriate security controls and implementing them
- monitoring the activities, making adjustments as necessary to address any issues, changes and improvement opportunities.

To standardize this discipline, academics and professionals collaborate to offer guidance, policies, and industry standards on password, antivirus software, firewall, encryption software, legal liability, security awareness and training, and so forth. This standardization may be further driven by a wide variety of laws and regulations that affect how data is accessed, processed, stored, transferred and destroyed. However, the implementation of any standards and guidance within an entity may have limited effect if a culture of continual improvement isn't adopted.

Various definitions of information security are suggested. For example:

"Information Security is a multidisciplinary area of study and professional activity which is concerned with the development and implementation of security mechanisms of all available types (technical, organizational, human-oriented and legal) in order to keep information in all its locations (within and outside the organization's perimeter) and, consequently, information systems, where information is created, processed, stored, transmitted and destroyed, free from threats.

TASK 2. Choose the correct answer:

1. What is a firewall in computer security?
    a. A type of virus
    b. A software program

c. A hardware device
d. A computer network security system

2. What is the main purpose of an antivirus program?
   a. To protect a computer from viruses and other malicious software
   b. To backup data on a computer
   c. To manage passwords
   d. To monitor network traffic

3. What is a strong password?
   a. A password containing only numbers
   b. A password that is easily guessed
   c. A password containing letters, numbers, and symbols
   d. A password containing only uppercase letters

4. What is a phishing attack?
   a. An attack that targets vulnerabilities in a computer's hardware
   b. A type of malware
   c. An attempt to steal sensitive information by pretending to be a trustworthy source
   d. A type of cyberattack that targets software vulnerabilities

5. What is the purpose of encryption?
   a. To scramble data so it can only be read by the intended recipient
   b. To speed up data transfer
   c. To protect data during transit
   d. To make data more organized

6. What is two-factor authentication?
   a. A security measure that requires two forms of identification before accessing a system
   b. A type of encryption
   c. A backup procedure
   d. A password manager

7. What is the purpose of a disaster recovery plan?
   a. To minimize the impact of a security breach
   b. To ensure that an organization can respond to a disaster or other emergency that affects information systems – and minimize the effect on business operations.
   c. To manage passwords
   d. To monitor network traffic

8. What is the difference between confidentiality, integrity, and availability in information security?
   a. Confidentiality means keeping information private, integrity means making sure information is accurate and trustworthy, and availability means making sure information is accessible when needed.
   b. Confidentiality means making sure information is accessible when needed, integrity means keeping information private, and availability means making sure information is accurate and trustworthy.

c. Confidentiality means making sure information is accurate and trustworthy, integrity means keeping information private, and availability means making sure information is accessible when needed.
d. Confidentiality means making sure information is accessible when needed, integrity means making sure information is accurate and trustworthy, and availability means keeping information private.

9. What is a man-in-the-middle attack?
   a. An attack where an attacker intercepts and potentially alters communication between two parties
   b. An attack where an attacker gains unauthorized access to a system by exploiting software vulnerabilities
   c. An attack where an attacker steals sensitive information by pretending to be a trustworthy source
   d. An attack where an attacker gains access to a system by guessing a password

10. What is social engineering in the context of information security?
    a. A technique used to trick individuals into revealing sensitive information
    b. A type of software program
    c. A security measure that requires two forms of identification before accessing a system
    d. A hardware device used to protect a network from unauthorized access

TASK 3. Elaborate on the measures to ensure information security.

Билет 6

TASK 1. Read the text and summarise it using the topic-related vocabulary.

At the core of information security is information assurance, the act of maintaining the confidentiality, integrity, and availability (CIA) of information, ensuring that information is not compromised in any way when critical issues arise. These issues include but are not limited to natural disasters, computer/server malfunction, and physical theft. While paper-based business operations are still prevalent, requiring their own set of information security practices, enterprise digital initiatives are increasingly being emphasized, with information assurance now typically being dealt with by information technology (IT) security specialists. These specialists apply information security to technology (most often some form of computer system). It is worthwhile to note that a computer does not necessarily mean a home desktop. A computer is any device with a processor and some memory. Such devices can range from non-networked standalone devices as simple as calculators, to networked mobile computing devices such as smartphones and tablet computers. IT security specialists are almost always found in any major enterprise/establishment due to the nature and value of the data within larger businesses. They are responsible for keeping all of the technology within the company secure from malicious cyber attacks that often attempt to acquire critical private information or gain control of the internal systems.

The field of information security has grown and evolved significantly in recent years. It offers many areas for specialization, including securing networks and allied infrastructure, securing applications and databases, security testing, information systems auditing, business continuity planning, electronic record discovery, and digital forensics. Information security professionals are very stable in their employment. As of 2013 more than 80 percent of professionals had no change in employer or employment over a period of a year, and the number of professionals is projected to continuously grow more than 11 percent annually from 2014 to 2019.

Threats

Information security threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, theft of identity, theft of equipment or information, sabotage, and information extortion. Viruses, worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the information technology (IT) field.

TASK 2. Choose the correct answer

1. What is a firewall in computer security?
   a. A type of virus
   b. A software program
   c. A hardware device
   d. A computer network security system

2. What is the main purpose of an antivirus program?
   a. To protect a computer from viruses and other malicious software
   b. To backup data on a computer
   c. To manage passwords
   d. To monitor network traffic

3. What is a strong password?
   a. A password containing only numbers
   b. A password that is easily guessed
   c. A password containing letters, numbers, and symbols
   d. A password containing only uppercase letters

4. What is a phishing attack?
   a. An attack that targets vulnerabilities in a computer's hardware
   b. A type of malware
   c. An attempt to steal sensitive information by pretending to be a trustworthy source
   d. A type of cyberattack that targets software vulnerabilities

5. What is the purpose of encryption?
   a. To scramble data so it can only be read by the intended recipient
   b. To speed up data transfer
   c. To protect data during transit
   d. To make data more organized

6. What is two-factor authentication?
   a. A security measure that requires two forms of identification before accessing a system
   b. A type of encryption
   c. A backup procedure
   d. A password manager

7. What is the purpose of a disaster recovery plan?
   a. To minimize the impact of a security breach
   b. To ensure that an organization can respond to a disaster or other emergency that affects information systems – and minimize the effect on business operations.
   c. To manage passwords
   d. To monitor network traffic

8. What is the difference between confidentiality, integrity, and availability in information security?
   a. Confidentiality means keeping information private, integrity means making sure information is accurate and trustworthy, and availability means making sure information is accessible when needed.
   b. Confidentiality means making sure information is accessible when needed, integrity means keeping information private, and availability means making sure information is accurate and trustworthy.
   c. Confidentiality means making sure information is accurate and trustworthy, integrity means keeping information private, and availability means making sure information is accessible when needed.
   d. Confidentiality means making sure information is accessible when needed, integrity means making sure information is accurate and trustworthy, and availability means keeping information private.

9. What is a man-in-the-middle attack?
   a. An attack where an attacker intercepts and potentially alters communication between two parties
   b. An attack where an attacker gains unauthorized access to a system by exploiting software vulnerabilities
   c. An attack where an attacker steals sensitive information by pretending to be a trustworthy source
   d. An attack where an attacker gains access to a system by guessing a password

10. What is social engineering in the context of information security?
    a. A technique used to trick individuals into revealing sensitive information
    b. A type of software program
    c. A security measure that requires two forms of identification before accessing a system
    d. A hardware device used to protect a network from unauthorized access

TASK 3. Elaborate on the main principles of network security.

Билет 7

TASK 1. Read the text and summarise it using the topic-related vocabulary.

Threats

Information security threats come in many different forms. Some of the most common threats today are software attacks, theft of intellectual property, theft of identity, theft of equipment or information, sabotage, and information extortion. Viruses,[39] worms, phishing attacks, and Trojan horses are a few common examples of software attacks. The theft of intellectual property has also been an extensive issue for many businesses in the information technology (IT) field.

Identity theft is the attempt to act as someone else usually to obtain that person's personal information or to take advantage of their access to vital information through social engineering. Theft of equipment or information is becoming more prevalent today due to the fact that most devices today are mobile, are prone to theft and have also become far more desirable as the amount of data capacity increases. Sabotage usually consists of the destruction of an organization's website in an attempt to cause loss of confidence on the part of its customers. Information extortion consists of theft of a company's property or information as an attempt to receive a payment in exchange for returning the information or property back to its owner, as with ransomware. There are many ways to help protect yourself from some of these

attacks but one of the most functional precautions is conduct periodical user awareness. The number one threat to any organisation are users or internal employees, they are also called insider threats.

Governments, military, corporations, financial institutions, hospitals, non-profit organisations, and private businesses amass a great deal of confidential information about their employees, customers, products, research, and financial status. Should confidential information about a business's customers or finances or new product line fall into the hands of a competitor or a black hat hacker, a business and its customers could suffer widespread, irreparable financial loss, as well as damage to the company's reputation. From a business perspective, information security must be balanced against cost; the Gordon-Loeb Model provides a mathematical economic approach for addressing this concern.

For the individual, information security has a significant effect on privacy, which is viewed very differently in various cultures.

TASK 2. Choose the correct answer

1. What is a firewall in computer security?
   a. A type of virus
   b. A software program
   c. A hardware device
   d. A computer network security system

2. What is the main purpose of an antivirus program?
   a. To protect a computer from viruses and other malicious software
   b. To backup data on a computer
   c. To manage passwords
   d. To monitor network traffic

3. What is a strong password?
   a. A password containing only numbers
   b. A password that is easily guessed
   c. A password containing letters, numbers, and symbols
   d. A password containing only uppercase letters

4. What is a phishing attack?
   a. An attack that targets vulnerabilities in a computer's hardware
   b. A type of malware
   c. An attempt to steal sensitive information by pretending to be a trustworthy source
   d. A type of cyberattack that targets software vulnerabilities

5. What is the purpose of encryption?
   a. To scramble data so it can only be read by the intended recipient
   b. To speed up data transfer
   c. To protect data during transit
   d. To make data more organized

6. What is two-factor authentication?
   a. A security measure that requires two forms of identification before accessing a system
   b. A type of encryption
   c. A backup procedure

d. A password manager

7. What is the purpose of a disaster recovery plan?
   a. To minimize the impact of a security breach
   b. To ensure that an organization can respond to a disaster or other emergency that affects information systems – and minimize the effect on business operations.
   c. To manage passwords
   d. To monitor network traffic

8. What is the difference between confidentiality, integrity, and availability in information security?
   a. Confidentiality means keeping information private, integrity means making sure information is accurate and trustworthy, and availability means making sure information is accessible when needed.
   b. Confidentiality means making sure information is accessible when needed, integrity means keeping information private, and availability means making sure information is accurate and trustworthy.
   c. Confidentiality means making sure information is accurate and trustworthy, integrity means keeping information private, and availability means making sure information is accessible when needed.
   d. Confidentiality means making sure information is accessible when needed, integrity means making sure information is accurate and trustworthy, and availability means keeping information private.

9. What is a man-in-the-middle attack?
   a. An attack where an attacker intercepts and potentially alters communication between two parties
   b. An attack where an attacker gains unauthorized access to a system by exploiting software vulnerabilities
   c. An attack where an attacker steals sensitive information by pretending to be a trustworthy source
   d. An attack where an attacker gains access to a system by guessing a password

10. What is social engineering in the context of information security?
    a. A technique used to trick individuals into revealing sensitive information
    b. A type of software program
    c. A security measure that requires two forms of identification before accessing a system
    d. A hardware device used to protect a network from unauthorized access

TASK 3. Elaborate on the main threats when using the internet. What can be done to avoid it?

Билет 8

TASK 1. Read the text and summarise it using the topic-related vocabulary.

Since the early days of communication, diplomats and military commanders understood that it was necessary to provide some mechanism to protect the confidentiality of correspondence and to have some means of detecting tampering. Julius Caesar is credited with the invention of the Caesar cipher c. 50 B.C., which was created in order to prevent his secret messages from being read should a message fall into the wrong hands. However, for the most part protection was achieved through the application of procedural handling controls. Sensitive information was marked up to indicate that it should be protected and transported by trusted persons, guarded and stored in a secure

environment or strong box. As postal services expanded, governments created official organizations to intercept, decipher, read, and reseal letters (e.g., the U.K.'s Secret Office, founded in 1653.

In the mid-nineteenth century more complex classification systems were developed to allow governments to manage their information according to the degree of sensitivity. For example, the British Government codified this, to some extent, with the publication of the Official Secrets Act in 1889. Section 1 of the law concerned espionage and unlawful disclosures of information, while Section 2 dealt with breaches of official trust. A public interest defense was soon added to defend disclosures in the interest of the state. A similar law was passed in India in 1889, The Indian Official Secrets Act, which was associated with the British colonial era and used to crack down on newspapers that opposed the Raj's policies. A newer version was passed in 1923 that extended to all matters of confidential or secret information for governance. By the time of the First World War, multi-tier classification systems were used to communicate information to and from various fronts, which encouraged greater use of code making and breaking sections in diplomatic and military headquarters. Encoding became more sophisticated between the wars as machines were employed to scramble and unscramble information.

The establishment of computer security inaugurated the history of information security. The need for such appeared during World War II. The volume of information shared by the Allied countries during the Second World War necessitated formal alignment of classification systems and procedural controls. An arcane range of markings evolved to indicate who could handle documents (usually officers rather than enlisted troops) and where they should be stored as increasingly complex safes and storage facilities were developed. The Enigma Machine, which was employed by the Germans to encrypt the data of warfare and was successfully decrypted by Alan Turing, can be regarded as a striking example of creating and using secured information. Procedures evolved to ensure documents were destroyed properly, and it was the failure to follow these procedures which led to some of the greatest intelligence coups of the war.

TASK 2. Choose the correct answer

1. What is a firewall in computer security?
   a. A type of virus
   b. A software program
   c. A hardware device
   d. A computer network security system

2. What is the main purpose of an antivirus program?
   a. To protect a computer from viruses and other malicious software
   b. To backup data on a computer
   c. To manage passwords
   d. To monitor network traffic

3. What is a strong password?
   a. A password containing only numbers
   b. A password that is easily guessed
   c. A password containing letters, numbers, and symbols
   d. A password containing only uppercase letters

4. What is a phishing attack?
   a. An attack that targets vulnerabilities in a computer's hardware
   b. A type of malware
   c. An attempt to steal sensitive information by pretending to be a trustworthy source
   d. A type of cyberattack that targets software vulnerabilities

5. What is the purpose of encryption?
   a. To scramble data so it can only be read by the intended recipient
   b. To speed up data transfer
   c. To protect data during transit
   d. To make data more organized

6. What is two-factor authentication?
   a. A security measure that requires two forms of identification before accessing a system
   b. A type of encryption
   c. A backup procedure
   d. A password manager

7. What is the purpose of a disaster recovery plan?
   a. To minimize the impact of a security breach
   b. To ensure that an organization can respond to a disaster or other emergency that affects information systems – and minimize the effect on business operations.
   c. To manage passwords
   d. To monitor network traffic

8. What is the difference between confidentiality, integrity, and availability in information security?
   a. Confidentiality means keeping information private, integrity means making sure information is accurate and trustworthy, and availability means making sure information is accessible when needed.
   b. Confidentiality means making sure information is accessible when needed, integrity means keeping information private, and availability means making sure information is accurate and trustworthy.
   c. Confidentiality means making sure information is accurate and trustworthy, integrity means keeping information private, and availability means making sure information is accessible when needed.
   d. Confidentiality means making sure information is accessible when needed, integrity means making sure information is accurate and trustworthy, and availability means keeping information private.

9. What is a man-in-the-middle attack?
   a. An attack where an attacker intercepts and potentially alters communication between two parties
   b. An attack where an attacker gains unauthorized access to a system by exploiting software vulnerabilities
   c. An attack where an attacker steals sensitive information by pretending to be a trustworthy source
   d. An attack where an attacker gains access to a system by guessing a password

10. What is social engineering in the context of information security?
    a. A technique used to trick individuals into revealing sensitive information
    b. A type of software program
    c. A security measure that requires two forms of identification before accessing a system
    d. A hardware device used to protect a network from unauthorized access

TASK 3. What kind of risks can you take dealing with Cloud Computing?

Билет 9

TASK 1. Read the text and summarise it using the topic-related vocabulary.

History

Various Mainframe computers were connected online during the Cold War to complete more sophisticated tasks, in a communication process easier than mailing magnetic tapes back and forth by computer centers. As such, the Advanced Research Projects Agency (ARPA), of the United States Department of Defense, started researching the feasibility of a networked system of communication to trade information within the United States Armed Forces. In 1968, the ARPANET project was formulated by Dr. Larry Roberts, which would later evolve into what is known as the internet.

In 1973, important elements of ARPANET security were found by internet pioneer Robert Metcalfe to have many flaws such as the: "vulnerability of password structure and formats; lack of safety procedures for dial-up connections; and nonexistent user identification and authorizations", aside from the lack of controls and safeguards to keep data safe from unauthorized access. Hackers had effortless access to ARPANET, as phone numbers were known by the public. Due to these problems, coupled with the constant violation of computer security, as well as the exponential increase in the number of hosts and users of the system, "network security" was often alluded to as "network insecurity".

The end of the twentieth century and the early years of the twenty-first century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller, more powerful, and less expensive computing equipment made electronic data processing within the reach of small business and home users. The establishment of Transfer Control Protocol/Internetwork Protocol (TCP/IP) in the early 1980s enabled different types of computers to communicate. These computers quickly became interconnected through the internet.

The rapid growth and widespread use of electronic data processing and electronic business conducted through the internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process, and transmit. The academic disciplines of computer security and information assurance emerged along with numerous professional organizations, all sharing the common goals of ensuring the security and reliability of information systems.

TASK 2. Choose the correct answer

1. What is a firewall in computer security?
   a. A type of virus
   b. A software program
   c. A hardware device
   d. A computer network security system

2. What is the main purpose of an antivirus program?
   a. To protect a computer from viruses and other malicious software
   b. To backup data on a computer
   c. To manage passwords
   d. To monitor network traffic

3. What is a strong password?
   a. A password containing only numbers
   b. A password that is easily guessed
   c. A password containing letters, numbers, and symbols
   d. A password containing only uppercase letters

4. What is a phishing attack?
   a. An attack that targets vulnerabilities in a computer's hardware
   b. A type of malware
   c. An attempt to steal sensitive information by pretending to be a trustworthy source
   d. A type of cyberattack that targets software vulnerabilities

5. What is the purpose of encryption?
   a. To scramble data so it can only be read by the intended recipient
   b. To speed up data transfer
   c. To protect data during transit
   d. To make data more organized

6. What is two-factor authentication?
   a. A security measure that requires two forms of identification before accessing a system
   b. A type of encryption
   c. A backup procedure
   d. A password manager

7. What is the purpose of a disaster recovery plan?
   a. To minimize the impact of a security breach
   b. To ensure that an organization can respond to a disaster or other emergency that affects information systems – and minimize the effect on business operations.
   c. To manage passwords
   d. To monitor network traffic

8. What is the difference between confidentiality, integrity, and availability in information security?
   a. Confidentiality means keeping information private, integrity means making sure information is accurate and trustworthy, and availability means making sure information is accessible when needed.
   b. Confidentiality means making sure information is accessible when needed, integrity means keeping information private, and availability means making sure information is accurate and trustworthy.
   c. Confidentiality means making sure information is accurate and trustworthy, integrity means keeping information private, and availability means making sure information is accessible when needed.
   d. Confidentiality means making sure information is accessible when needed, integrity means making sure information is accurate and trustworthy, and availability means keeping information private.

9. What is a man-in-the-middle attack?
   a. An attack where an attacker intercepts and potentially alters communication between two parties
   b. An attack where an attacker gains unauthorized access to a system by exploiting software vulnerabilities
   c. An attack where an attacker steals sensitive information by pretending to be a trustworthy source
   d. An attack where an attacker gains access to a system by guessing a password

10. What is social engineering in the context of information security?

a. A technique used to trick individuals into revealing sensitive information
b. A type of software program
c. A security measure that requires two forms of identification before accessing a system
d. A hardware device used to protect a network from unauthorized access

TASK 3. Speak about the phenomena of identity theft and availability attacks.

Билет 10

TASK 1. Read the text and summarise it using the topic-related vocabulary.

Confidentiality

In information security, confidentiality "is the property, that information is not made available or disclosed to unauthorized individuals, entities, or processes." While similar to "privacy," the two words are not interchangeable. Rather, confidentiality is a component of privacy that implements to protect our data from unauthorized viewers. Examples of confidentiality of electronic data being compromised include laptop theft, password theft, or sensitive emails being sent to the incorrect individuals.

Integrity

In IT security, data integrity means maintaining and assuring the accuracy and completeness of data over its entire lifecycle. This means that data cannot be modified in an unauthorized or undetected manner.This is not the same thing as referential integrity in databases, although it can be viewed as a special case of consistency as understood in the classic ACID model of transaction processing. Information security systems typically incorporate controls to ensure their own integrity, in particular protecting the kernel or core functions against both deliberate and accidental threats. Multi-purpose and multi-user computer systems aim to compartmentalize the data and processing such that no user or process can adversely impact another: the controls may not succeed however, as we see in incidents such as malware infections, hacks, data theft, fraud, and privacy breaches.

More broadly, integrity is an information security principle that involves human/social, process, and commercial integrity, as well as data integrity. As such it touches on aspects such as credibility, consistency, truthfulness, completeness, accuracy, timeliness, and assurance.

Availability

For any information system to serve its purpose, the information must be available when it is needed.This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. High availability systems aim to remain available at all times, preventing service disruptions due to power outages, hardware failures, and system upgrades.Ensuring availability also involves preventing denial-of-service attacks, such as a flood of incoming messages to the target system, essentially forcing it to shut down.

TASK 2. Choose the correct answer

1. What is a firewall in computer security?
   a. A type of virus
   b. A software program
   c. A hardware device
   d. A computer network security system

2. What is the main purpose of an antivirus program?
   a. To protect a computer from viruses and other malicious software

b. To backup data on a computer
c. To manage passwords
d. To monitor network traffic

3. What is a strong password?
   a. A password containing only numbers
   b. A password that is easily guessed
   c. A password containing letters, numbers, and symbols
   d. A password containing only uppercase letters

4. What is a phishing attack?
   a. An attack that targets vulnerabilities in a computer's hardware
   b. A type of malware
   c. An attempt to steal sensitive information by pretending to be a trustworthy source
   d. A type of cyberattack that targets software vulnerabilities

5. What is the purpose of encryption?
   a. To scramble data so it can only be read by the intended recipient
   b. To speed up data transfer
   c. To protect data during transit
   d. To make data more organized

6. What is two-factor authentication?
   a. A security measure that requires two forms of identification before accessing a system
   b. A type of encryption
   c. A backup procedure
   d. A password manager

7. What is the purpose of a disaster recovery plan?
   a. To minimize the impact of a security breach
   b. To ensure that an organization can respond to a disaster or other emergency that affects information systems – and minimize the effect on business operations.
   c. To manage passwords
   d. To monitor network traffic

8. What is the difference between confidentiality, integrity, and availability in information security?
   a. Confidentiality means keeping information private, integrity means making sure information is accurate and trustworthy, and availability means making sure information is accessible when needed.
   b. Confidentiality means making sure information is accessible when needed, integrity means keeping information private, and availability means making sure information is accurate and trustworthy.
   c. Confidentiality means making sure information is accurate and trustworthy, integrity means keeping information private, and availability means making sure information is accessible when needed.
   d. Confidentiality means making sure information is accessible when needed, integrity means making sure information is accurate and trustworthy, and availability means keeping information private.

9. What is a man-in-the-middle attack?
   a. An attack where an attacker intercepts and potentially alters communication between two parties
   b. An attack where an attacker gains unauthorized access to a system by exploiting software vulnerabilities
   c. An attack where an attacker steals sensitive information by pretending to be a trustworthy source
   d. An attack where an attacker gains access to a system by guessing a password

10. What is social engineering in the context of information security?
    a. A technique used to trick individuals into revealing sensitive information
    b. A type of software program
    c. A security measure that requires two forms of identification before accessing a system
    d. A hardware device used to protect a network from unauthorized access

TASK 3. Who are hackers? What motivates them? How do they conduct their attacks? How do they manage to breach the measures we have in place to ensure confidentiality, integrity, and availability? Which best practices can we adopt to defeat hackers?