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

УТВЕРЖДАЮ
И.о. директора института

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ
ФГБОУ ВО «КГТУ»
СВЕДЕНИЯ О СЕРТИФИКАТЕ ЭП
Сертификат:
4ae0684d0d529bb9d0248a5b51302ea1
Владелец: Гоконаев Мирослав Валерьевич
Действителен: с 02.08.2024 по 26.10.2025

Фонд оценочных средств
(приложение к рабочей программе дисциплины)

«ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ»

основной профессиональной образовательной программы специалитета
по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

«БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

ИНСТИТУТ	цифровых технологий
РАЗРАБОТЧИК	кафедра информационной безопасности

1 РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ, ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ И КРИТЕРИИ ОЦЕНИВАНИЯ

1.1 Результаты освоения дисциплины

Таблица 1 – Планируемые результаты обучения по дисциплине, соотнесенные с установленными компетенциями

Код и наименование компетенции	Дисциплина	Результаты обучения (владения, умения и знания), соотнесенные с компетенциями
ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства	Основы информационной безопасности	*Знать:* основные составляющие национальных интересов Российской Федерации в информационной сфере; сущность и понятие информационной безопасности, характеристику ее составляющих; цели, задачи, принципы и основные направления обеспечения информационной безопасности государства. *Уметь:* самостоятельно получать новые знания по предметной области и в областях, непосредственно примыкающих к объектам будущей профессиональной деятельности; самостоятельно получать знания из смежных областей науки и техники: углублять знания, уточнять по признакам понятий, отделять существенные признаки от несущественных, уточнять границы использования знаний. *Владеть:* технологиями систематизации и накопления научных знаний в предметной области.

1.2 К оценочным средствам текущего контроля успеваемости относятся:

- тестовые задания открытого и закрытого типов;

Промежуточная аттестация по дисциплине проводится в форме зачета, который выставляется по результатам прохождения всех видов текущего контроля успеваемости. При необходимости тестовые задания закрытого и открытого типов могут быть использованы для проведения промежуточной аттестации.

1.3 Критерии оценки результатов освоения дисциплины

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 (табл. 2).

Таблица 2 – 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 изучаемых объектов	Обладает частичными и разрозненными знаниями, которые не может научно- корректно связывать между собой (только некоторые из которых может связывать между собой)	Обладает минимальным набором знаний, необходимым для системного взгляда на изучаемый объект	Обладает набором знаний, достаточным для системного взгляда на изучаемый объект	Обладает полнотой знаний и системным взглядом 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, интерпретировать и систематизировать необходимую информацию в рамках поставленной задачи	Может найти, систематизировать необходимую информацию, а также выявить новые, дополнительные 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 предоставленной информации	В состоянии осуществлять систематический и научно корректный анализ предоставленной информации, вовлекает в исследование новые релевантные задаче данные	В состоянии осуществлять систематический и научно-корректный анализ предоставленной 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

1.4 Оценивание тестовых заданий закрытого типа осуществляется по системе зачтено/ не зачтено («зачтено» – 41-100% правильных ответов; «не зачтено» – менее 40 % правильных ответов) или пятибалльной системе (оценка «неудовлетворительно» - менее 40 % правильных ответов; оценка «удовлетворительно» - от 41 до 60 % правильных ответов; оценка «хорошо» - от 61 до 80% правильных ответов; оценка «отлично» - от 81 до 100 % правильных ответов).

Тестовые задания открытого типа оцениваются по системе «зачтено/ не зачтено». Оценивается верность ответа по существу вопроса, при этом не учитывается порядок слов в словосочетании, верность окончаний, падежи.

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ОПК-1: Способен оценивать роль информации, информационных технологий и информационной безопасности в современном обществе, их значение для обеспечения объективных потребностей личности, общества и государства

Тестовые задания открытого типа:

1 Защита информации –

Эталонный ответ: деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию.

2. Криптографическая защита информации –

Эталонный ответ: защита информации с помощью ее криптографического преобразования.

3 Физическая защита информации –

Эталонный ответ: защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

4 Способ защиты информации –

Эталонный ответ: порядок и правила применения определенных принципов и средств защиты информации.

5 Защита информации, направленная на предотвращение неконтролируемого распространения защищаемой информации в результате ее разглашения и несанкционированного доступа к ней, а также на исключение (затруднение) получения защищаемой информации [иностранными] разведками и другими заинтересованными субъектами –

Эталонный ответ: защита информации от утечки

6 Защита информации, направленная на предотвращение несанкционированного доступа и воздействия на защищаемую информацию с нарушением установленных прав и (или) правил на изменение информации, приводящих к разрушению, уничтожению, искажению, сбою в работе, незаконному перехвату и копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации –

Эталонный ответ: защита информации от несанкционированного воздействия

7 Защита информации, направленная на предотвращение несанкционированного доведения защищаемой информации до заинтересованных субъектов (потребителей), не имеющих права доступа к этой информации.

Эталонный ответ: защита информации от разглашения

8 Защита информации, направленная на предотвращение получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации –

Эталонный ответ: защита информации от несанкционированного доступа защита информации от несанкционированного доступа

9 Защита информации, направленная на предотвращение преднамеренного воздействия, в том числе электромагнитного и (или) воздействия другой физической природы, осуществляемого в террористических или криминальных целях –

Эталонный ответ: защита информации от преднамеренного воздействия

10 Защита информации от [иностранной] разведки –

Эталонный ответ: защита информации, направленная на предотвращение получения защищаемой информации [иностранной] разведкой.

11 Основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность осуществления технических и организационных мероприятий, необходимых для достижения цели защиты информации –

Эталонный ответ: замысел защиты информации.

12 Цель защиты информации –

Эталонный ответ: заранее намеченный результат защиты информации.

13 Совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации –

Эталонный ответ: система защиты информации

14 Безопасность информации (данных) –

Эталонный ответ: состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность.

15 Объект защиты информации –

Эталонный ответ: информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с целью защиты информации.

16 Информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации –

Эталонный ответ: защищаемая информация.

17 Физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин –

Эталонный ответ: носитель защищаемой информации.

18 Защищаемый объект информатизации –

Эталонный ответ: объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

19 Информационная система, предназначенная для обработки защищаемой информации с требуемым уровнем ее защищенности –

Эталонный ответ: защищаемая информационная система.

20 Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации –

Эталонный ответ: угроза (безопасности информации).

21 Явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней –

Эталонный ответ: фактор, воздействующий на защищаемую информацию

22 Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации –

Эталонный ответ: источник угрозы безопасности информации.

23 Свойство информационной системы, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации –

Эталонный ответ уязвимость (информационной системы); брешь.

24 Модель угроз (безопасности информации) –

Эталонный ответ: физическое, математическое, описательное представление свойств или характеристик угроз безопасности информации.

Тестовые задания закрытого типа:

1. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на …

А) соблюдение норм международного права в сфере информационной безопасности

Б) выявление нарушителей и привлечение их к ответственности

В) разработку методов и усовершенствование средств информационной безопасности

Г) соблюдение конфиденциальности информации ограниченного доступа

2. Информация, составляющая государственную тайну, не может иметь гриф…

А) «для служебного пользования»

Б) «секретно»

В) «совершенно секретно»

Г) «особой важности»

3. Одной из основных угроз доступности информации является:

А) злонамеренное изменение данных

Б) хакерская атака

В) непреднамеренные ошибки пользователей

Г) перехват данных

4. Что не относится к компьютерной преступности?

а) подделка компьютерной информации

б) хищение информации

в) распространение вирусов

г) согласованное копирование данных

5. Как называется комплекс мероприятий, направленных на обеспечение информационной безопасности?

а) защитой информации

б) авторизацией

в) информационной безопасностью

г) безопасным состоянием

6. Кто отвечает за защиту автоматизированной системы от несанкционированного доступа к информации?

а) пользователь

б) аутентификатор

в) авторизатор

г) администратор защиты

7. Перехват данных является угрозой…

а) доступности

б) целостности

в) конфиденциальности

г) для администратора

8. Сбор и накопление информации о событиях, происходящих в информационной системе, называется…

а) протоколированием

б) аудитом

в) экранированием

г) криптографией

3 ТИПОВЫЕ ЗАДАНИЯ НА КОНТРОЛЬНУЮ РАБОТУ, КУРСОВУЮ РАБОТУ/КУРСОВОЙ ПРОЕКТ, РАСЧЕТНО-ГРАФИЧЕСКУЮ РАБОТУ

В данном разделе по учебному плану типовые задания на контрольную работу, курсовую работу/курсовой проект, расчётно-графическую работу не предусмотрены.

4 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

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

Преподаватель – разработчик – А.Г. Жестовский.

Фонд оценочных средств рассмотрен и одобрен методической комиссией института цифровых технологий (протокол №5 от 29.08.2024 г).

Председатель методической комиссии  О.С. Витренко