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)

«ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ»

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 – 8 Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах	Защита информации от утечки по техническим каналам	Знать: технические каналы утечки информации, возможности технических разведок, Уметь: анализировать и оценивать угрозы информационной безопасности объекта; пользоваться нормативными документами по защите информации. Владеть: методами и средствами выявления угроз безопасности автоматизированным системам; методами технической защиты информации.
ОПК – 9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации		Знать: способы и средства защиты информации от утечки по техническим каналам. Уметь: применять отечественные и зарубежные стандарты в области безопасности для проектирования, разработки и оценки защищенности автоматизированных систем Владеть: методами формирования требований по защите информации; методами расчета и инструментального контроля показателей технической защиты информации.

1.2 К оценочным средствам текущего контроля успеваемости относятся:

- тестовые задания открытого и закрытого типов.

К оценочным средствам для промежуточной аттестации относятся:

- экзаменационные задания по дисциплине, представленные в виде тестовых заданий закрытого и открытого типов.

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 – 8 Способен применять методы научных исследований при проведении разработок в области защиты информации в автоматизированных системах

Тестовые задания открытого типа:

1. Комплекс организационных и технических мероприятий, в результате которых подтверждается соответствие системы защиты информации объекта информатизации требованиям безопасности информации

Эталонный ответ: аттестация объектов информатизации

2. Безопасность информации –

Эталонный ответ: состояние защищенности информации, при котором обеспечены ее конфиденциальность, доступность и целостность;

3. Технические средства и системы, не предназначенные для передачи, обработки и хранения секретной информации, устанавливаемые совместно с основными техническими средствами и системами

Эталонный ответ: вспомогательные технические средства и системы

4. Совокупность действий, направленных на применение организационных мер и программно-технических способов защиты информации на объекте информатизации

Эталонный ответ: организационно-технические мероприятия по обеспечению защиты информации

5. Распространение информации –

Эталонный ответ: действия, направленные на получение информации неопределенным кругом лиц или передачу информации неопределенному кругу лиц;

6. Помещение, в котором проводятся секретные работы и/или хранятся в нерабочее время носители сведений, составляющих государственную тайну

Эталонный ответ: режимное помещение

7. Обеспечение некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Эталонный ответ: техническая защита информации

8. Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Эталонный ответ: физическая защита информации

9. 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:

10. Защита информации от [иностранной] разведки:

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

11. 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

12. Объект информатизации, предназначенный для обработки защищаемой информации с требуемым уровнем ее защищенности.

Эталонный ответ: защищаемый объект информатизации

13. Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Эталонный ответ: угроза (безопасности информации):

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

Эталонный ответ: источник угрозы безопасности информации

15. Уязвимость (информационной системы); брешь:

Эталонный ответ: свойство информационной системы, обусловливающее возможность реализации угроз безопасности, обрабатываемой в ней информации.

Тестовые задания закрытого типа:

1. В течение какого срока ФСТЭК принимает решение о выдаче лицензии на техническую защиту конфиденциальной информации после получения документов от соискателя?

20 дней

35 дней

45 дней

10 дней

2. На какой срок выдается лицензия на техническую защиту конфиденциальной информации?

1 год

5 лет

3 года

бессрочная

3. Кто осуществляет сертификацию средств защиты информации в области криптографической защиты информации?

ФСБ России

МВД России

Роскомнадзор

ФСТЭК России

4. Как называются опасные сигналы, которые создаются техническим средством обработки информации для выполнения заданных функций?

случайные

намеренные

функциональные

демаскирующие

5. Как называется сигнал, который передает защищаемую информацию и может быть перехвачен злоумышленником с дальнейшим извлечением этой информации?

информационный

демаскирующий

опасный

функциональный

6. Как называются закладки, использующие для передачи информации силовые линии?

радиозакладки

ИК-передатчики

сетевые закладки

стетоскопы

7. Какое средство чаще всего используется злоумышленником для снятия информации в виброакустическом канале утечки?

стетоскоп

анализатор спектра

микрофон

лазер

8. Как называется микрофон, представляющий из себя фазированную акустическую решетку, в узлах которой размещаются микрофоны?

трубчатый микрофон

параболический микрофон

плоский микрофон

проводной микрофон

9. Количество звуковой энергии, проходящей за единицу времени через единицу площади, называется:

интенсивность звука

громкость слуха

звуковое давление

уровень силы звука

10. Что использует “телефонное ухо” для передачи информации злоумышленнику?

силовую линию

радиоканал

телефонную линию

оптический канал

ОПК – 9 Способен решать задачи профессиональной деятельности с учетом текущего состояния и тенденций развития информационных технологий, средств технической защиты информации, сетей и систем передачи информации

Тестовые задания открытого типа:

1. Воздействие на защищаемую информацию с нарушением установленных прав и (или) правил доступа, приводящее к утечке, искажению, подделке, уничтожению, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации.

Эталонный ответ: несанкционированное воздействие на информацию

2. Несанкционированное воздействие на информацию, осуществляемое путем применения источника электромагнитного поля для наведения (генерирования) в автоматизированных информационных системах электромагнитной энергии с уровнем, вызывающим нарушение нормального функционирования (сбой в работе) технических и программных средств этих систем.

Эталонный ответ: преднамеренное силовое электромагнитное воздействие на информацию:

3. Средства защиты информации, в том числе средства физической защиты информации, криптографические средства защиты информации, средства контроля эффективности защиты информации, средства и системы управления, предназначенные для обеспечения защиты информации.

Эталонный ответ: техника защиты информации

4. Техническое, программное, программно-техническое средство, вещество и (или) материал, предназначенные или используемые для защиты информации.

Эталонный ответ: средство защиты информации

5. Средство защиты информации, предназначенное или используемое для контроля эффективности защиты информации.

Эталонный ответ: средство контроля эффективности защиты информации:

6. Средство защиты информации, предназначенное или используемое для обеспечения физической защиты объекта защиты информации.

Эталонный ответ: средство физической защиты информации

7. Исследование, проводимое в целях выявления технических каналов утечки защищаемой информации и оценки соответствия защиты информации (на объекте защиты) требованиям нормативных и правовых документов в области безопасности информации.

Эталонный ответ: специальное исследование (объекта защиты информации)

8. Постоянное наблюдение за процессом обеспечения безопасности информации в информационной системе с целью установить его соответствие требованиям безопасности информации.

Эталонный ответ: мониторинг безопасности информации

9. Рассмотрение документа по защите информации физическим или юридическим лицом, имеющим право на проведение работ в данной области, с целью подготовить соответствующее экспертное заключение.

Эталонный ответ: экспертиза документа по защите информации

10. Систематическое использование информации для выявления угроз безопасности информации, уязвимостей информационной системы и количественной оценки вероятностей реализации 10 угроз с использованием уязвимостей и последствий реализации угроз для информации и информационной системы, предназначенной для обработки этой информации.

Эталонный ответ: анализ информационного риска

11. Общий процесс анализа информационного риска и его оценивания.

Эталонный ответ: оценка информационного риска

12. Эффективность защиты информации:

Эталонный ответ: степень соответствия результатов защиты информации цели защиты информации.

13. Установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации, или допустимое значение показателя эффективности защиты информации.

Эталонный ответ: требование по защите информации:

14. Показатель эффективности защиты информации:

Эталонный ответ: мера или характеристика для оценки эффективности защиты информации.

15. Значение показателя эффективности защиты информации, установленное нормативными и правовыми документами

Эталонный ответ: норма эффективности защиты информации.

Тестовые задания закрытого типа:

1. Как называется шум с тенденцией спада спектральной плотности 3 дБ на октаву в сторону высоких частот?

белый шум

речеподобная помеха

розовый шум

серый шум

2. Для подавления диктофонов используют генераторы мощных шумовых сигналов … диапазона частот.

миллиметрового

метрового

сантиметрового

дециметрового

3. Как называются акустоэлектрические преобразователи, в которых под воздействием акустической волны возникают эквивалентные электрические сигналы?

активные

электрические

пассивные

емкостные

4. Какой режим работы сканирующего приемника будет использовать потенциальный злоумышленник, если знает, на каких частотах работают интересующие его приборы?

режим сканирования слепых зон

режим автоматического сканирования по фиксированным частотам

ручной режим работы

режим автоматического сканирования в заданном диапазоне частот

5. Какой компонент комплекса для перехвата радиосигналов предназначен для определения параметров сигнала (частота, вид модуляции, структура кода и т.п.)?

радиоприемник

анализатор технических характеристик сигнала

радиопеленгатор

антенна

регистрирующее устройство

6. На какие две категории делятся акустоэлектрические преобразователи по физическим процессам, порождающим опасные сигналы?

пассивные

электрические

акустические

активные

7. Какое устройство позволяет принимать и анализировать структуру сигнала в широком диапазоне частот?

сканирующий приемник

анализатор спектра

интерсептер

радиотестер

8. Как называется способ защиты информации от утечки через ПЭМИН, основанный на локализации электромагнитной энергии в определенном пространстве за счет ограничения распространения ее всеми возможными способами?

зашумление

экранирование

ослабление

магнитострикция

9. Какая характеристика сканирующего приемника может привести к увеличению количества ложных срабатываний?

скорость сканирования

количество каналов

габариты

чувствительность

10. В основу работы, какого устройства контроля положено изменение плотности среды вокруг радиозакладки?

тепловизор

металлодетектор

анализатор спектра

радиочастотометр

11. Какой показатель используется для оценки защищенности речевой информации?

информативность

разборчивость речи

звуковое давление

коэффициент затухания

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 «Защита информации от утечки по техническим каналам» представляет собой компонент основной профессиональной образовательной программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация Безопасность открытых информационных систем).

Разработчик – доцент кафедры «Информационная безопасность» — 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