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)

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ»

основной профессиональной образовательной программы специалитета
по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

«ИНФОРМАЦИОННАЯ 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-5.1: Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем; ОПК-5.2: Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем.	Информационная безопасность открытых информационных систем	**Знать:** - концепцию диспетчера доступа; методы и средства ограничения доступа к ресурсам распределенной ВС; методы и средства обнаружения уязвимостей распределенной ВС; методы и средства обнаружения атак на ресурсы распределенной ВС; методы и средства противодействия атакам на ресурсы распределенной ВС. **Уметь:** организовывать защиту распределенной ВС; производить защиту от атак на ресурсы распределенной ВС; производить защиту программ от изменений в распределенной ВС; осуществлять контроль трафика в рамках распределенной ВС. **Владеть:** средствами защиты в распределенной ВС от несанкционированного доступа и нарушения функциональности ее подсистем; средствами борьбы с атаками злоумышленников на ресурсы серверов баз данных; методикой контроля информационной целостности в распределенной ВС

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.

Промежуточная аттестация в форме зачета проходит по результатам прохождения всех видов текущего контроля успеваемости. В отдельных случаях (при не прохождении всех видов текущего контроля) зачет может быть проведен в виде тестирования.

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	В состоянии осуществлять научно корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно корректный анализ предоставленной	В состоянии осуществлять систематический и научно-корректный анализ предо-

Система оценок / Критерий	2	3	4	5
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
	только некоторые из имеющихся у него сведений		информации, вовлекает в исследование новые релевантные задаче данные	ставленной 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

Компетенция ОПК-5.1: Способен разрабатывать и реализовывать политику информационной безопасности открытых информационных систем;

Тестовые задания открытого типа:

1. Открытой распределенной информационной системой (open distributed information system) называется система, располагающая службами, пользование которыми возможно при использовании стандартных_____

Ответ: синтаксиса и семантики

2. Угроза это:

Ответ: совокупность условий и факторов, определяющих потенциальную или реально существующую опасность возникновения инцидента, который может привести к нанесению ущерба изделию ИТ или его владельцу.

3. Определите класс автоматизированной системы по следующим классификационным признакам: многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. И все пользователи имеют равные права доступа ко всей информации АС, обрабатывается “Служебная тайна” и общедоступная информация:

Ответ: 2Б

4. Методы и средства защиты информации бывают: _____ и_____.

Ответ: технические; программные

5. _____ -это параметр, характеризующий возможность нанесения описываемой системе повреждений любой природы теми или иными внешними средствами или факторами.

Ответ: Уязвимость

6. Для определения доступности хоста может использоваться простейшая команда:

Ответ: Ping

7. Укажите два основных метода анализа, связанных с выявлением атак в системах обнаружения вторжений (СОВ):

Ответ: сигнатурный метод и метод, связанный с выявлением аномального поведения

8. _____(англ.)-это разновидность программ, представляющих собой некую ловушку для злоумышленников, которая помогает отследить атаки и подобрать эффективные методы для борьбы с ними

Ответ: Honeypots

9. Укажите тип троянских утилит, с помощью которых осуществляется кража паролей:

Ответ: Trojan-PSW.

10. Укажите тип троянских утилит несанкционированных обращений к интернет-ресурсам:

Ответ: Trojan-Clicker.

11. Укажите тип троянских утилит, предназначенных для несанкционированного пользователем сбора адресов электронной почты на компьютере с последующей передачей их злоумышленнику через электронную почту, HTTP, FTP или другими способами:

Ответ: Trojan-Mailfinder.

12. Проработка инцидентов, связанных с нарушением безопасности интрасети, включает следующие шаги:

Ответ: защита компьютерной системы; идентификация проблемы; ослабление проблемы; устранение проблемы; устранение последствий происшествия и выполнение последовательного анализа

13. _____ это приложение или последовательность команд, предназначенная для реализации каких-либо уязвимостей операционной системы или специализированного программного обеспечения.

Ответ: Эксплойт

14. Атаки типа IP-spoofing – это атаки на _____ уровне

Ответ: сетевом

15. Межсетевой экран _____ нежелательный трафик

Ответ: блокирует

16. Атака на веб-приложения типа XSS происходит на _____ уровне.

Ответ: прикладном

17. Атака SQL-Injection происходит на _____ уровне.

Ответ: прикладном

18. Атака IP-spoofing – это:

Ответ: подмена реального IP-адреса ложным в отправляемых пакетах.

19. Укажите стандартный порт протокола HTTPS:

Ответ: 443

20. Прослушивание трафика в локальных сетях производится с помощью специальных программ:

Ответ: снифферов

21. Смысл атаки ICMP Redirect состоит:

Ответ: в навязывании атакуемому хосту ложного маршрутизатора;

22. Политика безопасности в отношении интрасети организации должна складывается из трех основных составляющих:

Ответ: положений и инструкций, определяющих правила работы персонала с защищаемой информацией, сетевыми программными и аппаратными средствами

23. Аудит и мониторинг работы интрасети осуществляется из единого центра, занимающегося выполнением задач защиты, и предназначен:

Ответ: помочь определить и оценить общее состояние системы защиты информации и защищенности интрасети организации; помочь обнаружить несоответствия (рассогласованности) в интрасети; собрать информацию для анализа атак на интрасеть; проверить соответствие между политикой безопасности и мерами ее осуществляющими;

24. В зависимости от типа МЭ ядро МЭ **НЕ** может быть реализовано_____

Ответ: таблицей прерываний

Тестовые задания закрытого типа:

25. В этом порядке задаются права доступа в ОС Linux:

1. группа-владелец- остальные

3. владелец-группа-остальные

2. остальные-владелец-группа

4.остальные-группа-владелец

26. В системе поблочного отображения адресов виртуальной памяти указываются:

1. блок, в котором расположен этот элемент, и смещение элемента относительно начала блока

3. адрес элемента в таблице отображения блоков процесса**.**

2. адрес файла подкачки и номер блока в этом файле, в котором расположен указанный элемент

4. адрес реальной памяти, в котором расположен указанный элемент

27. Как соотносятся контекст и дескриптор процесса:

1. дескриптор содержит более оперативную информацию, которая должна быть легко доступна подсистеме планирования процессов, а контекст используется операционной системой для восстановления прерванного процесса

3. это одно и то же

2. дескриптор включает в себя контекст

4. контекст включает в себя дескриптор

28. Что из перечисленного **НЕ** является состоянием процесса?

1. порождение
3. прерывание
2. выполнение
4. готовность

29. Определите класс автоматизированной системы по следующим классификационным признакам: *АС, в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности, обрабатывается "Комерческая тайна".*

1. 2Б
3. 1Д
2. 1Г
4. 3Б

30. Среди множества компонентов, образующих СОВ, отсутствуют:

1. модуль агрегирования
3. модуль хранения
2. модуль анализа
4. данные

31. Смысл атаки ICMP Redirect состоит:

1. в навязывании атакуемому хосту ложного маршрутизатора
3. в навязывании атакуемому хосту ложной сети;
2. в шифровании траффика, обеспечивающего утечку данных
4. в создании ложного маршрутизатора;

32. Запрещение прохождения пакета выполняется одним из следующих способов:

1. отсылается предупреждение отправителю пакета
3. пакет отбрасывается (drop) без каких-либо дополнительных действий
2. пакет отбрасывается (reject) и отправителю посылается пакет с установленным флагом «сброс соединения».
4. пакет отбрасывается и отправителю посылается сообщения ICMP-хост недостижим или порт недоступен.

Компетенция ОПК-5.2: Способен разрабатывать и эксплуатировать системы защиты информации открытых информационных систем;

Тестовые задания открытого типа:

1. Обладатель информации это:

Ответ: лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам;

2. Рассчитайте уровень защищенности ПДн для ИС, если в ней обрабатываются биометрические ПДн и актуальны угрозы второго типа, обрабатываются персональные данные сотрудников:

Ответ: УЗ 2

3. Документом, определяющим лицензируемые виды деятельности, является

Ответ: Федеральный закон от 25. 12. 2023 г. № 99-ФЗ «О лицензировании отдельных видов деятельности»;

4. Средства защиты от НСД какого класса по РД СВТ минимально достаточны для обеспечения любого уровня защищенности персональных данных:

Ответ: 5

5. Аттестация ФСТЭК является обязательной для организаций, которые работают в _____. В таких организациях также недопустимо использование несертифицированного ПО

Ответ: в ГИС, АСУ ТП, относятся к объектам КИИ, обрабатывают ПДн и государственную тайну.

6. Условием доработки функционирующих информационных систем является_____

Ответ: изменение класса или уровня защищенности информационной системы

7. Формирование требований к защите информации, содержащейся в информационной системе, согласно 17 приказа ФСТЭК, осуществляется _____ информации.

Ответ: обладателем

8. Основные требования к содержанию системы защиты персональных данных, при автоматизированной обработке, определяют следующие документы:

Ответ: ФЗ 152; ППРФ 1119; Приказ ФСТЭК №21;

9. «Специальные проверки» (спецпроверки) это:

Ответ: проверки технических средств иностранного и совместного производства на наличие возможно внедренных электронных устройств перехвата информации.

10. «Специальные исследования (специсследования)» это:

Ответ: выявление с помощью контрольно-измерительной аппаратуры возможных каналов утечки информации ограниченного доступа, обрабатываемой техническими средствами

11. Активными способами защиты информации являются:

Ответ: создание маскирующих электромагнитных помех в посторонних проводниках и соединительных линиях технических средств;

12. Контроль состояния защиты информации отраслевыми и федеральными органами заключается в оценке:

Ответ: соблюдения требований нормативно-методических документов по защите информации

13. Влияют ли угрозы недекларированных возможностей на уровень защищенности ИСПДн

Ответ: Да, для системного и прикладного ПО

14. В процессе создания автоматизированных систем допускается исключать следующую стадию:

Ответ: эскизную

15. В процессе создания автоматизированных систем этапы: " выполнение работ в соответствии с гарантийными обязательствами" и "послегарантийное обслуживание" входят в стадию:

Ответ: сопровождение автоматизированной системы

16. Порядок стадий создания автоматизированных систем (АС) выглядит следующим образом:

Ответ: 1) формирование требований к АС; 2) разработка концепции АС; 3) техническое задание; 4) эскизный проект; 5) технический проект; 6) рабочая документация; 7) ввод в действие; 8) сопровождение АС

17. _____ - мера доверия, которая может быть оказана архитектуре, инфраструктуре, программно-аппаратной реализации системы и методам управления её конфигурацией и целостностью

Ответ: Гарантированность безопасности

18. Совокупность требований к конкретной разработке, выполнение которых обеспечивает достижение поставленных целей безопасности – это _____-

Ответ: задание по безопасности

19. Имитация целевых атак злоумышленников и выявление уязвимости инфраструктуры называется:

Ответ: пентест

20. Соответствие по профилю защиты средств антивирусной защиты информации (САВЗ) типа А, Б, В, Г

1	А – САВЗ	А	применяемые для централизованного администрирования средствами, антивирусной защиты, установленными на компонентах информационных систем;
2	Б – САВЗ	Б	применяемые на серверах информационных систем;
3	В – САВЗ	В	применяемые на автоматизированных рабочих местах информационных систем;
4	Г – САВЗ	Г	применяемые на автономных автоматизированных рабочих местах.

Эталонный ответ**: 1а; 2б; 3в; 4г**

21. Порядок разработки модели угроз определяется документом:

Ответ: ФСТЭК России. Методический документ. Методика оценки угроз безопасности информации (5 февраля 2021 г.)

22. Процесс получения качественной и количественной оценок уровня защиты информации, основанных на полученной информации об информационной системе организации и последующим ее анализе, а также разработка плана устранения выявленных уязвимостей информационной системы называется...

Ответ: аудит

23. Укажите соответствие нормативно-правовых актов (НПА) и их названий

1	№152-ФЗ	А	"О персональных данных"

2	Приказ ФСТЭК №21	Б	"Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных"
3	ПП №1119	В	"Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных"
4	Приказ ФСТЭК №17	Г	"Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах"

Эталонный ответ: **1а; 2б; 3в; 4г**

24. _____автоматизированной системы – это совокупность организационных мероприятий, технических, программных и программно-технических средств защиты информации и средств контроля эффективности защиты информации.

Ответ: Средства защиты информации

Тестовые задания закрытого типа:

25. Средствами защиты информации, подлежащими сертификации, являются:

1. Средства контроля эффективности применения средств защиты информации

3.Средства защиты информации (технические, программные, программно-технические) от НСД, блокировки доступа и нарушения целостности

2. Средства контроля эффективности прочности ограждений

4.Строительные материалы, используемые для отделки помещений в которых размещаются отдельные элементы ИСПДн

26. К рекомендуемым методам и способам защиты информации в информационных системах относятся:

1. методы и способы защиты информации от несанкционированного доступа

2. методы и способы устранения конкурентов

3. методы и способы сокрытия информации от внутренних нарушителей

4. методы и способы защиты информации от утечки по техническим каналам.

27. К средствам контроля защищенности информации от НСД относятся:

1. средства формирования и контроля полномочий доступа в информационных (автоматизированных) системах;

3.сканеры безопасности

2. межсетевые экраны

4. антивирусные средства

28. Для контроля защищенности информации применяются средства

1. Рекомендованные ФСБ России;

2. Рекомендованные Роскомнадзором;

3. Рекомендованные ФСТЭК России

4. прошедшие в установленном законом порядке процедуру оценки соответствия

29. Соответствие классов ГИС и уровня защищённости ИСПДн

1	1 класс	А	Уровни 2,3,4
2	2 класс	Б	Уровни 1,2,3,4
3	3 класс	В	Уровни 3,4

Эталонный ответ: **1б, 2а, 3в**

30. Информация по категории доступа классифицируется как:

1. Общедоступная

3. Ограниченного доступа

2. Конфиденциальная

4. Особо конфиденциальная

31. Что такое ACL?

1 список управления доступом

3. средство для хранения паролей

2. сценарий входа в систему

4.инструмент мандатного управления доступом в ОС

32. Что из перечисленного **НЕ** содержится в маркере доступа пользователя?

1. уровень доступа пользователя в системе

3. идентификатор пользователя

2. привилегии пользователя

4.идентификатор сеанса работы пользователя, к которому относится маркер доступа

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

Преподаватель-разработчик - доцент, к.ф.-м.н. Н.Я.Великите

Фонд оценочных средств рассмотрен и одобрен методической комиссией института цифровых технологий (протокол №5 от 29 августа 2024 г).

Председатель методической комиссии  О.С. Витренко