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 модуля)

«ПРОГРАММНО-АППАРАТНЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ»

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-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем	Программно-аппаратные средства защиты информации	*Знание:* основные средства и способы обеспечения безопасности информации, принципы построения систем защиты информации; программно-аппаратные средства обеспечения защиты информации автоматизированных систем; способы реализации угроз безопасности в автоматизированных системах. *Умения:* проводить выбор и настройку программно-аппаратных средств обеспечения безопасности информации для использования их в составе автоматизированной системы с целью обеспечения требуемого уровня защищенности автоматизированной системы. *Навыки:* обоснования и внедрения перечня сертифицированных и несертифицированных средств защиты информации, необходимых для создания системы защиты информации автоматизированной системы.

1.2 К оценочным средствам текущего контроля успеваемости относятся:

- тестовые задания открытого и закрытого типов.

К оценочным средствам для промежуточной аттестации относятся:

- типовые задания по курсовому проекту;

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

Промежуточная аттестация в форме дифференцированного зачета (зачета с оценкой) 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 только некоторые	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 предоставленной ин-

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

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ОПК-15. Способен осуществлять администрирование и контроль функционирования средств и систем защиты информации автоматизированных систем, инструментальный мониторинг защищенности автоматизированных систем

Тестовые задания закрытого типа:

1. Среди множества компонентов, образующих СОВ, отсутствуют:

1. данные.
2. модуль анализа.
3. модуль хранения.
4. модуль реакции.
5. **модуль агрегирования.**

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

1. **Trojan-PSW.**
2. Trojan-Downloader.
3. Rootkit.
4. Trojan-GameThief.
5. Trojan-Banker.

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

1. Backdoor.
2. Trojan-Spy.
3. **Trojan-Clicker.**
4. Trojan-Downloader.
5. Trojan-Mailfinder.

4. Укажите троянские утилиты сокрытого присутствия в операционной системе:

1. Backdoor.
2. Trojan-Spy.
3. Trojan-Clicker.
4. **Rootkit.**

5. 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:

1. Trojan-Clicker.
2. Rootkit.
3. Trojan-GameThief.
4. Trojan-Banker.
5. **Trojan-Mailfinder.**

6. Семейство электронных ключей HASP не включает в свой состав следующие модели:

1. HASP4.
2. MemoHASP.
3. TimeHASP.
4. **SetHASP.**

7. Резервное копирование не может быть:

1. полным
2. возобновляемым
3. выборочным
4. **асинхронным**

8. Аутентификация в защищенных АС **НЕ** может осуществляться методом:

1. парольная аутентификация (ввод специальной индивидуальной для каждого пользователя последовательности символов на клавиатуре);

2. на основе биометрических измерений;

3. на основе поведенческого контроля;

4. с использованием физических носителей аутентифицирующей информации.

Тестовые задания открытого типа:

9. Уязвимость информации — это:

Ответ: Событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

10. Распределенные атаки затруднительно обнаружить по следующим указанным причинам: _____

Ответ: отсутствие корреляции данных, скрытые сигнатуры, при блокировании источника обнаруженной атаки на межсетевом экране могут быть заблокированы сети, которые должны быть доступны для атакуемых хостов, трудно определить истинного нарушителя безопасности**.**

11. Тип троянских утилит, предназначенных для кражи пользовательской информации, относящейся к сетевым играм, имеет название:

Ответ: Trojan-GameThief.

12. Тип троянских утилит, предназначенных для кражи пользовательской информации, относящейся к банковским системам, имеет название:

Ответ: Trojan-Banker.

13. Эксплойт – это:

Ответ: приложение или последовательность команд, предназначенная для реализации каких-либо уязвимостей операционной системы или специализированного программного обеспечения.

14. Программная закладка, работающая по принципу модели «перехват» **внедряется в** долговременную память компьютера и хранимые в этой памяти**:**

Ответ: программные средства.

15. Программная закладка, работающая по принципу модели троянский конь» **внедряется в:**
Ответ: в постоянно используемое ПО.

16. Программная закладка, работающая по принципу модели «наблюдатель» **осуществляет контроль за**:
Ответ: процессами обработки информации в компьютерной системе.

17. Программная закладка, работающая по принципу модели «искажение» или инициатор ошибок, искажает:
Ответ: потоки данных, возникающие при работе прикладных программ.

18. Программной закладка, работающая по принципу модели «перехват» в скрытой области внешней памяти прямого доступа, сохраняет:
Ответ: фрагменты вводимой и выводимой информации.

19. Политика безопасности в отношении интрасети организации должна складывается из трех составляющих, а именно:
Ответ:
a) планов защиты отдельных подсистем;
b) планов защиты отдельных ресурсов;
c) положений и инструкций, определяющих правила работы персонала с защищаемой информацией, сетевыми программными и аппаратными средствами;

20. Укажете два метода анализа, связанных с выявлением атак в СОВ:
Ответ: сигнатурный метод и метод, связанный с выявлением аномального поведения;

21. Аудит и мониторинг работы интрасети осуществляется из единого центра, занимающегося выполнением задач защиты, и предназначен для:
Ответ: оценки общего состояния системы защиты информации и защищенности интрасети организации, проверки соответствия между политикой безопасности и мерами ее осуществляющими.

22. Политика безопасности в системе (сети) – это комплекс:

Ответ: руководств, требований обеспечения необходимого уровня безопасности

23. В классификацию вирусов по способу заражения входят

Ответ: резидентные, нерезидентные вирусы

24. Вирусы, изменяющие порядок своих команд, называют:

Ответ: метаморфные вирусы

25. Вредоносные программы, которые используют rootkit-технологии для внедрения в ОС и сокрытия своего присутствия, имеют название:
Ответ: троянские программы.

26. Полиморфный вирус – это:

Ответ: вирус, способный менять порядок и состав своего байт-кода при каждом новом цикле заражения.

27. Принципы работы многофакторной аутентификации в АС/ИС состоят в следующем:

Ответ: при осуществлении аутентификации передача каждого «фактора» (аутентифицирующей информации) происходит по независимым или раздельным каналам, что сокращает возможности нарушителя по перехвату этого сеанса обмена целиком.

28. Механизмы (политики) разграничения доступа, которые применяются в современных СЗИ, следующие:

Ответ: дискреционный механизм (на основе матрицы с детальным указанием сторон и возможностей работы с объектами), мандатный механизм (на основе уровней и меток конфиденциальности), либо комбинированный подход.

29. Модули, которые используются в ОС Linux в механизмах идентификации и аутентификации, называются:

Ответ: подключаемые модули аутентификации (PAM - Pluggable Authentication Modules).

30. ACL используется для:

Ответ: разграничения доступа субъектов к объектам.

31. Биометрический вектор – это:

Ответ: набор биометрических признаков, используемых для идентификации субъекта.

32. Системы SIEM используются для:

Ответ: контроля событий безопасности информационной системе организации

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

Учебным планом предусмотрен курсовой проект. Иные типы работ данного раздела не предусматриваются

Курсовой проект направлен на закрепление полученных теоретических знаний и приобретение умений и навыков в области выполнения настроек, эксплуатации средств ЗИ, поиска вредоносных объектов в ИС.

Тема 1. **Разработка скриптов AVZ для удаления и восстановления системы после заражения вирусными объектами**

Цель: разработка и тестирование скриптов для средства AVZ (Anti-Virus Zaitsev), которые будут способствовать поиску, удалению и восстановлению системы после заражения вирусными объектами, такими как троян, червь и вирус.

Задачи проекта:

1. Изучение средства AVZ:

– Изучить средство AVZ и его функциональные возможности;

– Определение специфики структуру и синтаксис языка скриптов AVZ;

2. Разработка скриптов для поиска и удаления вредоносных объектов:

– Разработать скрипты, которые будут выполнять поиск вредоносных объектов на компьютерной системе;

– Обеспечить возможность удаления обнаруженных объектов;

3. Тестирование скриптов:

– Провести тестирование разработанных скриптов на тестовых вирусных объектах;

– Оценить эффективность скриптов в обнаружении и удалении вирусных объектов;

4. Заключение и рекомендации:

– Подвести итоги выполненной работы, оценить её результаты;

– Предоставить рекомендации по дальнейшему развитию и совершенствованию скриптов для борьбы с вирусами.

Тема 2. **Определение координат защищаемого устройства при помощи GPS датчика**

Возможности сочетания технологий сети, и современных датчиков позволяет обрабатывать большое количество информации, собранной системами IoT. Эта информация позволяет автоматизировать процессы ранее требующий вмешательство человека..

Цель: создание устройства для отслеживания и оповещения об изменении положения защищаемого объекта.

Задачи:

– изучение технологии интернет вещей;
– изучение возможностей GPS и GSM модулей;
– изучение функционала MQTT сервера;
– изучение способа шифрования GSM трафика

Тема 3. **Разработка инструментария для анализа вредоносного кода**

Цель: разработка программного модуля, который выполняет функции отслеживания всех процессов запущенных на компьютере (используя dump-памяти), поиск процессов по всем каталогам, анализ программы для вывода информации о том является ли она вредоносной, использование инструментов для отладки и анализа вредоносной программы.

Задачи:

– изучение того, что из себя представляет вредоносное ПО;
– изучение для чего используется анализ вредоносных программ;
– рассмотрение уже существующих программных средств для анализа системы;
– проектирования программного модуля использованием Python

4 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «Программно-аппаратные средства защиты информации» представляет собой компонент основной профессиональной образовательной программы специалитета по специальности 10.05.03 Информационная безопасность автоматизированных систем (специализация Безопасность открытых информационных систем).

Преподаватель-разработчик – В.В. Подтопельный

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

Председатель методической комиссии  О.С. Витренко