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)

«БЕЗОПАСНОСТЬ ОПЕРАЦИОННЫХ СИСТЕМ»

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-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем	Безопасность операционных систем	Знание: Способы реализации угроз безопасности в операционных системах; Способы реализации угроз безопасности в автоматизированных системах. Умения: формировать перечень мероприятий по предотвращению угроз безопасности операционных систем, информации в операционных системах Навыки: Обладает навыками выявления уязвимости информационно-технологических ресурсов автоматизированных систем; Обладает навыками определения комплекса мер (правил, процедур, практических приемов, руководящих принципов, методов, средств) для защиты операционных систем

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 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 только некоторые	В состоянии осуществлять научно корректный анализ предоставленной информации	В состоянии осуществлять систематический и научно корректный анализ предоставленной информации, во-	В состоянии осуществлять систематический и научно-корректный анализ предоставленной информации, вовле-

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		влекает в исследование новые релевантные задаче данные	кает 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-12. Способен применять знания в области безопасности вычислительных сетей, операционных систем и баз данных при разработке автоматизированных систем

Тестовые задания закрытого типа:

1. Из перечисленного не является основными функциями ОС:
a) диспетчеризация (планирование обработки задач);
b) распределение памяти между различными задачами;
c) распределение задачам необходимых ресурсов ВС;
d) обеспечение доверенной загрузки;

2. Режимы обработки данных существуют в ОС:
a) однопрограммные
b) параллельные
c) мультипрограммные
d) смешанные

3. Наличие многоуровневого планирования при организации работы ОС является следствием:
a) частотного принципа
b) принципа модульности
c) принципа функциональной избирательности
d) принципа функциональной избыточности

4. В состав системы защиты информации от НСД входят:
a) подсистема управления доступом
b) подсистема контроля за устройствами ввода/вывода информации
c) подсистема регистрации и учёта
d) подсистема обеспечения целостности

5. Из перечисленного **НЕ** является состоянием процесса:
a) порождение
b) выполнение
c) прерывание
d) готовность

6. Из перечисленного **НЕ** содержится в маркере доступа пользователя:
a) идентификатор пользователя
b) привилегии пользователя
c) идентификатор сеанса работы пользователя, к которому относится маркер доступа
d) уровень доступа пользователя в системе

7. Из перечисленного **НЕ** является требованием к подсистеме регистрации и учета:
a) использование идентификационного и аутентификационного механизма
b) запрос на доступ к защищаемому ресурсу (открытие файла, запуск программы и т.д.)
c) обеспечение доверенной загрузки ОС
d) действия по изменению ПРД

8. Файловая система, которая поддерживает хранение на диске дескрипторов защиты для файлов – это:
a) FAT32
b) NTFS
c) FAT16
d) HPFS

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. “Несанкционированный доступ к информации” это:
Ответ: доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств

11. Прерывание - это:
Ответ: временное прекращение процесса, вызванное событием, внешним по отношению к этому процессу, и совершенное таким образом, что процесс может быть продолжен

12. Как соотносятся контекст и дескриптор процесса:

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

13. В системе поблочного отображения адресов виртуальной памяти указываются:

Ответ: блок, в котором расположен этот элемент, и смещение элемента относительно начала блока

14. Порядок прав доступа в ОС Linux – это:

Ответ: владелец-группа-остальные

15. Тупиковая ситуация для процесса – это:

Ответ: ситуация, когда процесс ожидает некоторого события, которое никогда не произойдет

16. Кто в ОС может получить доступ к любому объекту по методу ACCESS_SYSTEM_SECURITY:

Ответ: аудитор

17. Домен безопасности – это:

Ответ: собрание участников безопасности, имеющих единый центр, использующий единую базу, единую групповую и локальную политики, ограничение времени работы учётной записи и прочие параметры, значительно упрощающие работу системного администратора организации, если в ней эксплуатируется большое число компьютеров

.

18. PAM– это:

Ответ: набор открытых библиотек подключаемых модулей аутентификации

19. Укажите для чего используется программа Iptables в ОС Linux:

Ответ: используется для управления встроенным брандмауэром netfilter.

20. Маркер доступа Windows идентифицирует:

Ответ: субъектов-пользователей системы

21. Каждому объекту системы, включая файлы, принтеры, сетевые службы, контейнеры Active Directory и другие, присваивается дескриптор безопасности, который определяет права доступа к объекту и содержит следующие основные атрибуты:

Ответ:

SID владельца, идентифицирующий учетную запись пользователя-владельца объекта;

пользовательский список управления доступом (Discretionary Access Control List, DACL), который позволяет отслеживать права и ограничения, установленные владельцем данного объекта. DACL может быть изменен пользователем, который указан как текущий владелец объекта;

системный список управления доступом (System Access Control List, SACL), определяющий перечень действий над объектом, подлежащих ауди-ту;

флаги, задающие атрибуты объекта.

22. Укажите, что означает переменная S в идентификаторе защиты (Security Identifiers, SID) объекта ОС Windows:

Ответ: неизменный идентификатор строкового представления SID.

23. Все действующие в системе объекты (пользователи, группы, локальные компьютеры, домены) идентифицируются в Windows по:

Ответ: по **идентификаторам защиты (Security Identifiers, SID)**

24. Поясните, что означает переменная **R** в идентификаторе защиты (Security Identifiers, SID) объекта ОС Windows**:**

Ответ: уровень ревизии (версия) системы.

25. Укажите, какой идентификатор содержит переменная **I** в идентификаторе защиты (Security Identifiers, SID) объекта ОС Windows **- это:**

Ответ: идентификатор полномочий.

26. Укажите, что содержит переменная **Sn** в идентификаторе защиты (Security Identifiers, SID) объекта ОС Windows**:**

Ответ: 32-битные коды (колчеством 0 и более) субагентов, которым было передано право выдать SID;

27. Укажите, какой идентификатор находится в переменной RID в идентификаторе защиты (Security Identifiers, SID) объекта ОС Windows**:**

Ответ: идентификатор уникального объекта безопасности в области, для которой был определен SID.

28. В DACL каждый ACE состоит из четырех частей, укажите их:

Ответ:

пользователи или группы,

права доступа,

данные о предоставление прав или изъятии,

набор флагов, определяющих, как данная запись будет наследоваться вложенными объектами (актуально, например, для папок файловой системы, разделов реестра);

29. Укажите, что выполняет команда ***mount*** в ОС Linux:

Ответ: монтирует файловые системы

30. Укажите, что выполняет команда ***chmod*** в ОС Linux

Ответ: выполняет установку атрибутов прав доступа к объекту

31. Поясните, для чего используется ***ps*** **в** ОС Linux.

Ответ: для отображения информации о текущих процессах в ОС Linux

32. Поясните, для чего используется ***chown*** **в** ОС Linux.
Ответ: изменение владельца файла в ОС Linux

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

Курсовая работа направлена на закрепление полученных теоретических знаний и приобретение умений и навыков в области выполнения настроек, эксплуатации средств ЗИ, поиска вредоносных объектов в ОС.

Типовое задание 1. Сетевая безопасность ос через netfilter в LINUX

Цель углубление знаний в области компьютерных сетей и операционных систем, изучение работы netfilter в ОС Linux.

Задачи работы:

1. Исследовать специфику интеграции правил сетевой безопансоти в ОС LINUX
2. Настроить правила фильтрации пакетов с помощью утилиты iptables.
3. Провести имитацию атаки на ОС LINUX.
4. Разработать алгоритм отражения атаки, отразить атаку, используя настройку межсетевого экрана.

Типовое задание 2. Исследование стойкости защитных процессов unix

Цель: изучение организации управления доступом в Unix системе, осуществление несанкционированного доступа к учётным данным, попытка изменения полномочий пользователя при несанкционированном доступе.

Задачи курсовой работы:

1. Исследовать ОС Unix;
2. Изучить основы организации ОС Unix;
3. Ознакомиться со средствами обеспечения безопасности в ОС- Unix при идентификации и аутентификации;
4. Изучить специфику несанкционированного доступа с возможностью изменения прав пользователей.

Типовое задание 3. Аудит ОС Linux (syslog)

Цель: обеспечение безопасности операционной системы путем настройки аудита файловой системы CentOS 7 на базе ОС Linux и настройка syslog (в CentOS 7 его аналог – rsyslog) для отслеживания действий пользователей и системы в целом.

Задачами в данной работе является:

1. Установить и настроить систему аудита ОС Linux auditd.
2. Провести ряд мероприятий, связанных с аудитом системы и подключения syslog, а именно:

2.1. Подключение записи файлов в syslog.

2.2. Просмотр доступа к файлам.

2.3. Мониторинг системных вызовов.

2.4. Запись событий безопасности.

2.5. Поиск событий.

2.6. Провести атаку по SSH и проверить, как на это отреагирует аудит.

3. Сделать выводы о работе системы аудита ОС Linux

Выполнив поставленные задачи, мы обеспечим нашу операционную систему рабочей и готовой к использованию службой аудита с системой записи лог-файлов.

4 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «Безопасность операционных 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 – 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