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)

«Программирование средств 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-7. Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ	Программирование средств защиты информации	*Знание*: способы и средства разработки компонентов систем защиты информации; основные информационные технологии, используемые в автоматизированных системах; национальные, межгосударственные и международные стандарты в области защиты информации, применяемые при разработке средств защиты информации. *Умения:* разрабатывать части проектной документации на системы защиты автоматизированных систем; работать в среде программирования, которая поддерживает изучаемый язык; настраивать инструментальные средства программирования языка высокого уровня для наиболее удобного для себя интерфейса. *Навыки:* владения основными средствами и методами разработки алгоритмов; владения приемами структурного программирования;

		владения технологиями и методами разработки программных приложений; анализа характера обрабатываемой информации и определение перечня информации, подлежащей защите; разработки отчетных документов и разделов технических заданий; обоснования перечня сертифицированных 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 курсовой работе;

- 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	**2**	**3**	**4**	**5**
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
Критерий	**«не зачтено»**	**«зачтено»**		
1 Системность и полнота зна-	Обладает частичными и разрозненными знаниями, которые не может	Обладает минимальным набором знаний, необходи-	Обладает набором знаний, достаточным для системного	Обладает полнотой знаний и системным взглядом

Система оценок	2	3	4	5
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
Критерий	**«не зачтено»**	**«зачтено»**		
ний в отношении изучаемых объектов	научно- корректно связывать между собой (только некоторые из которых может связывать между собой)	мым для системного взгляда на изучаемый объект	взгляда на изучаемый объект	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

2 ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕЙ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

ОПК-7. Способен создавать программы на языках общего назначения, применять методы и инструментальные средства программирования для решения профессиональных задач, осуществлять обоснованный выбор инструментария программирования и способов организации программ

Тестовые задания закрытого типа:

1. Для безопасной передачи данных в интернете используется протокол:

а) HTTP

б) FTP

c) HTTPS

d) SMTP

Ответ: c) HTTPS

2. Хеш-функции используются для следующего метода аутентификации:

a) Парольная аутентификация

b) Двухфакторная аутентификация

c) Аутентификация по сертификату

d) Аутентификация по отпечатку пальца

Ответ: a) Парольная аутентификация

3. Выберете из приведенных методов шифрования симметричный метод:

a RSA

b) AES

c) ECC

d) DSA

Ответ: B) AES

4. Укажете, подход к программированию средств защиты информации, который подразумевает использование метода "чёрного ящика" для тестирования

a) Тестирование на основе спецификаций

b) Тестирование на основе кода

c) Интеграционное тестирование

d) Регрессионное тестирование

Ответ: a) Тестирование на основе спецификаций

5. Укажите инструмент, который используется для управления и хранения криптографических ключей.

a) Keylogger

b) HSM (Hardware Security Module)

c) VPN

d) Firewall

Ответ: b) HSM (Hardware Security Module)

6. Подход к программированию средств защиты информации, который включает в себя регулярное обновление и патчинг программного обеспечения, называется

a) Программирование с нуля

b) Безопасная разработка

c) Инкрементальная разработка

d) Agile-разработка

Ответ: b) Безопасная разработка

7. Укажите алгоритм, который используется для генерации ключей в асимметричной криптографии

a) DES

b) Diffie-Hellman

c) Blowfish

d) RC4

Ответ: B) Diffie-Hellman

8. Укажите метод, который используется для шифрования данных в C++.

a) std::сортировать

b) std::хэш

c) OpenSSL

d) std::vector

Ответ: c) OpenSSL

Тестовые задания открытого типа:

9. Алгоритм _____ является асимметричным и использует пару ключей: открытый и закрытый.

Ответ: RSA

10. Метод Диффи-Хеллмана позволяет двум сторонам безопасно обмениваться ключами через _____

Ответ: открытый канал связи

11. Для генерации случайных чисел в криптографических приложениях на C++ без использования стандартного генератора псевдослучайных чисел, используется метод___

Ответ: random_device

12. Использование _____ позволяет защитить данные при передаче по сети путем их шифрования.

Ответ: SSL/TLS

13. Для обеспечения конфиденциальности данных при их передаче по сети используется _____.

Ответ: шифрование

14. В многопоточных приложениях гонка данных возникает, когда несколько потоков___

Ответ: одновременно пытаются получить доступ к общему ресурсу без надлежащей синхронизации

15. Ошибки приведения типов (Type Confusion) могут возникать, когда объект неправильно интерпретируется как другой тип, что может привести к _____

Ответ: нарушению целостности памяти и безопасности программы.

16. Отсутствие проверки границ при работе с массивами и контейнерами может привести к_____

Ответ: переполнению буфера или доступу к неинициализированной памяти

17. Ошибки синхронизации возникают при неправильном использовании _____

Ответ: мьютексов и других средств синхронизации

18. Использование неинициализированных переменных приводит к_____

Ответ: неопределённому поведению программы и уязвимостям в системе безопасности

19. Неправильное использование указателей, в том числе разыменование нулевых или неинициализированных указателей приводит к_____

Ответ: сбоям и уязвимостям в программе

20. Отсутствие проверки и фильтрации входных данных приводит к появлению уязвимостей, и, следовательно, требуется проверять и очищать_____

Ответ: все входные данные перед их использованием.

21. Статический анализ кода позволяет проверять исходный код на наличие_____ без его выполнения.

Ответ: потенциальных уязвимостей

22. Динамическое тестирование включает выполнение программы с целью выявления уязвимостей в _____ времени.

Ответ: реальном

23. Аудит конфигурации в АСУТП подразумевает проверку _____

Ответ: настроек системы и сетевых устройств на предмет безопасности.

24. Для защиты от SQL-инъекций в приложениях на C++, разработчики должны использовать _____ или _____.

Ответ: параметризованные запросы или подготовленные выражения.

25. В процессе разработки защищенного программного обеспечения на C++, использование принципа "защита по умолчанию" подразумевает, что _____.

Ответ: все настройки безопасности должны быть активированы по умолчанию.

26. Для защиты от атак с использованием вредоносного кода в приложениях на C++, необходимо реализовать механизмы _____.

Ответ: проверки целостности файлов и регулярного обновления антивирусных баз.

27. Использование механизма цифровых подписей в C++ позволяет обеспечить _____.

Ответ: аутентичность и целостность передаваемых данных

28. Crypto++ — это библиотека с открытым исходным кодом, предназначенная для_____

29. Ответ: криптографических операций.

30. Poco C++ — это набор библиотек для разработки_____

Ответ: разработки сетевых и интернет-приложений на C++.

31. Функция strcpy копирует строку из одного буфера в другой без проверки размера целевого буфера, что создает угрозу_____

Ответ: переполнения буфера.

32. Умные указатели, такие как std::unique_ptr и std::shared_ptr, обеспечивают автоматическое управление___

Ответ: памятью и предотвращают утечки ресурсов.

33. Использование стандартных контейнеров (например, std::vector, std::string) вместо массивов фиксированной длины позволяет избежать _____

Ответ: переполнения буфера

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

Учебным планом предусмотрена курсовая работа. Иные типы работ данного раздела не предусмотрены учебным планом

Курсовая работа направлена на закрепление полученных теоретических знаний и приобретение умений и навыков в области выполнения разработки средств ЗИ для ИС.

Тема 1. Разработка программы для удаления и восстановления системы после заражения вирусными объектами

Цель: разработка и тестирование программ, которые будут способствовать поиску, удалению и восстановлению системы после заражения вирусными объектами, такими как троянская программа, червь и вирус.

Задачи проекта:

– разработать программ, которые будут выполнять поиск вредоносных объектов на компьютерной системе;

– обеспечить возможность удаления обнаруженных объектов;

– провести тестирование разработанных программ на тестовых вирусных объектах;

– оценить эффективность программ в обнаружении и удалении вирусных объектов;

– подвести итоги выполненной работы, оценить её результаты;

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

Тема 2. Разработка программ 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.

Задачи:

–изучение того, что из себя представляет вредоносное ПО;

–изучение специфики анализа вредоносных программ;

–рассмотрение уже существующих программных средств для анализа системы;

–проектирования программного модуля с использованием выбранного языка программирования;

–подвести итоги выполненной работы, оценить её результаты;

–предоставить рекомендации по дальнейшему развитию и совершенствованию способов защиты информации.

Тема 3. Поиск и удаление вредоносных объектов из DOCX и PDF файлов

Цель: рассмотреть методы и приемы с использованием скриптов Python в Kali Linux для выявления вредоносных файлов и предотвращения нанесения ущерба системы вредоносными файлами.

Задачи:

– рассмотреть PDF и DOCX документы;

– проанализировать вредоносные документы (PDF и DOCX, содержащие вредоносные включения) с помощью различных утилит;

– выявить вредоносные объекты;

– попытаться извлечь вредоносные объекты;

– исследовать спецификацию и сигнатуру вредоносных объектов.

– подвести итоги выполненной работы, оценить её результаты;

− предоставить рекомендации по дальнейшему развитию и совершенствованию способов защиты

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