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)

«ТЕОРИЯ АНАЛИЗА КОМПЬЮТЕРНЫХ АТАК»

основной профессиональной образовательной программы специалитета
по специальности

10.05.03 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Специализация

"БЕЗОПАСНОСТЬ ОТКРЫТЫХ ИНФОРМАЦИОННЫХ СИСТЕМ"

ИНСТИТУТ	цифровых технологии
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-13: Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем	Теория анализа компьютерных атак	Знания: 1. Способы поиска и анализа уязвимостей 2. Методы учета уязвимостей, метрические спецификации уязвимостей и угроз 3. Методы моделирования компьютерных атак и их исследование и методы анализа компьютерных атак Умения: 1. Осуществлять поиск уязвимостей 2. Использовать методы определения метрических характеристик уязвимостей 3. Моделировать компьютерные атаки и анализировать, и прогнозировать с учетом специфики информационных систем и нарушителей Навыки: 1. Владеть навыком поиска и анализа уязвимостей, угроз 2. Определения специфических характеристик атак с учетом особенностей информационных систем 3. Владеть навыкам анализа компьютерных атак различными методами

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 по дисциплине проводится в форме зачета, который выставляется по результатам прохождения всех видов текущего контроля успеваемости и курсового проекта. При необходимости тестовые задания закрытого и открытого типов могут быть использованы для проведения промежуточной аттестации.

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

Система оценок / Критерий	2	3	4	5
	0-40%	**41-60%**	**61-80 %**	**81-100 %**
	«неудовлетворительно»	**«удовлетворительно»**	**«хорошо»**	**«отлично»**
	«не зачтено»	**«зачтено»**		
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

Компетенция ОПК-13: Способен организовывать и проводить диагностику и тестирование систем защиты информации автоматизированных систем, проводить анализ уязвимостей систем защиты информации автоматизированных систем.

Тестовые задания открытого типа (1 семестр):

1. Потенциальные возможности использования уязвимостей актива или группы активов конкретной угрозой для причинения ущерба организации это:_____

Ответ: риски информационной безопасности

2. Совокупность условий и факторов, создающих опасность нарушения информационной безопасности называют: _____

Ответ: угрозой информационной безопасности

3. Суммарный риск информационной безопасности определяется как:

Ответ: математическое ожидание ущерба (сумма произведений вероятностей каждого из негативных событий на величины потерь от них)

4. Направленный граф, вершины которого соответствуют стадиям атаки, в ребра – переходам между стадиями – это_____

Ответ: Граф компрометации

5. Нахождение путей атаки с минимальным временем означает: _____

Ответ: оценку максимального риска

6. К постоянным составляющим времени успешной атаки относятся:_____

Ответ: длительность разведки и нанесения ущерба

7. Экономический эффект от реализации контрмеры оценивается по формуле (граф атак):

Ответ: ROI=((ALE*RM)-CSI)/CSI

8. RM в расчёте графа атак обозначает:

Ответ: коэффициент уменьшения риска в результате реализации контрмеры

9. При трехфакторной оценке риска учитываются показатели:

Ответ: вероятность проявления угрозы, вероятность успешной эксплуатации уязвимостей, стоимость компонента и коэффициент актуальности ресурса

10. Совокупность организационных и инженерно-технических мер, направленных на защиту вашего бизнеса от разглашения и утечки информации, несанкционированного доступа (как к самой информации, так и на территорию охранного объекта) это:

Ответ: комплексная система информационной безопасности

11. Модуль, который служит для создания копий всех информационных данных на основной и резервный секретный сервер называется:

Ответ: модуль резервного копирования

12. Комплексность системы защиты информации достигается:

Ответ: охватом всех возможных угроз и согласованием между собой разнородных методов и средств, обеспечивающих защиту всех элементов предприятия

13. Подсистема, предназначенная для управления процессами защиты информации на основе законодательства и регламентации правил и порядка доступа к защищаемой информации и контроля всех процессов со стороны руководства организации и службы защиты информации называется:

Ответ: подсистема управления

14. Обязанности и права руководителей предприятия по вопросам защиты информации должны быть отражены в:

Ответ: должностных инструкциях

15. Опишите основные этапы анализа компьютерной атаки:

Ответ: может варьироваться, включает: сбор данных, анализ, идентификация уязвимостей, оценка ущерба и рекомендации по защите

16. Меры, которые можно предпринять для предотвращения атак на компьютерные системы:

Ответ: может включать: регулярное обновление ПО, использование антивирусов, обучение сотрудников, настройка брандмауэров и систем IDS

17. Системы обнаружения вторжений (IDS) используются для:

Ответ: может варьироваться, включает: мониторинг сетевого трафика и системных событий для выявления подозрительной активности

18. Опишите атаку «человек по середине»:

Ответ: атака, при которой злоумышленник получает доступ к каналу связи между легитимными сторонами (пользователями, приложениями, сетевыми устройствами и т. д.), что позволяет ему просматривать содержимое всех передаваемых ими сообщений, удалять и изменять их.

19. Вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям называется:

Ответ: фишинг

20. Целенаправленное воздействие программных и (или) программно-аппаратных средств на информационный ресурс в целях нарушения и (или) прекращения его функционирования и

(или) создания угрозы безопасности обрабатываемой таким ресурсом информации это:

Ответ: компьютерная атака

21. Если сайт или веб-приложение собирает у пользователей текстовую информацию (например, запрашивает логин и пароль), злоумышленник может ввести в поле ввода вредоносный запрос, который называется:

Ответ: SQL-инъекция

22. При этом виде атаки злоумышленники внедряют вредоносные скрипты в незащищённые сайты и веб-приложения:

Ответ: XSS (cross-site scripting) — межсайтовый скриптинг

Тестовые задания закрытого типа (1 семестр):

23. Метод, используемый для обнаружения атак в компьютерных системах:

1. Социальная инженерия
2. Физическая безопасность
3. Обучение персонала
4. **Статистический анализ**

24. Признаком атаки на компьютерную систему не является:

1. Необычная активность в сети
2. Увеличение трафика на сервере
3. **Регулярные резервные копии данных**
4. Неправильные учетные записи пользователей

25. Тип атаки подразумевающий использование уязвимостей программного обеспечения:

1. **Эксплуатация уязвимостей**
2. Социальная инженерия
3. DDOS-атака
4. Физическая атака

26. Метод шифрования, являющийся асимметричным:

1. AES
2. DES
3. **RSA**
4. Blowfish

27. Криптографический хеш это:

1. Метод шифрования данных
2. **Функция, преобразующая данные в фиксированную длину для обеспечения целостности**
3. Процесс дешифрования информации
4. Программа для создания паролей

28. Метод, используемый для предотвращения атак типа "человек посередине" (MITM):

1. Использование антивирусного ПО
2. Регулярные обновления системы
3. **Шифрование соединений с помощью SSL/TLS**
4. Настройка брандмауэра

29: Тип вредоносного ПО, имеющий возможность самовоспроизводиться и распространяться на другие системы:

1. **Вирус**
2. Троян
3. Шпионское ПО
4. Руткит

30: Пентест (penetration testing) это:

1. **Процесс тестирования системы на уязвимости путем имитации атаки**
2. Анализ сетевого трафика
3. Метод шифрования данных
4. Обучение сотрудников безопасности

Тестовые задания открытого типа (2 семестр):

1**.** Любое событие, которое может привести к компрометации конфиденциальности, целостности или доступности информации это:_____

Ответ: инцидент безопасности

2. Основные этапы процесса анализа инцидента безопасности (действия необходимые на каждом этапе): _____

Ответ: - сбор данных: сбор логов, сетевых данных и другой информации о инциденте.
- анализ: определение типа атаки, источника и масштаба.
- идентификация уязвимостей: поиск уязвимостей, которые были использованы злоумышленником.
- оценка ущерба: оценка влияния инцидента на организацию.
- рекомендации: разработка мер по предотвращению подобных инцидентов в будущем.
- отчетность: подготовка отчета о инциденте для заинтересованных сторон

3. Ключевые компоненты эффективной стратегии управления рисками информационной безопасности:

Ответ: - идентификация рисков: определение потенциальных угроз и уязвимостей.
- оценка рисков: анализ вероятности и воздействия рисков.
- управление рисками: принятие мер по уменьшению, передаче или избеганию рисков.
- мониторинг и пересмотр: регулярный пересмотр стратегии и мониторинг новых угроз

4. Основные признаки атаки DDoS:_____

Ответ: резкое увеличение трафика, замедление работы сервера, недоступность сервисов

5. Последствия утечки данных для компании: _____

Ответ: финансовые потери, штрафы и ухудшение репутации

6. Защита данных в облаке включает в себя:_____

Ответ: шифрование, использование многофакторной аутентификации и регулярные резервные копии

7. Основные принципы управления рисками:

Ответ: идентификация, оценка, управление и мониторинг рисков

8. Набор правил и процедур, направленных на защиту информации в организации:

Ответ: политика безопасности

9. Системы, которые мониторят сетевой трафик и анализируют его на предмет подозрительной активности и атак:

Ответ: методы обнаружения вторжений (IDS)

10. Основные группы методов обнаружения атак это:

Ответ: поведенческие методы, методы на основе знаний, сигнатурный анализ и методы интеллектуального анализа данных

11. Метод, который использует известные шаблоны поведения атак для выявления угроз, широко применяемый в коммерческих IDS называется:

Ответ: сигнатурный анализ

12. Преимущества поведенческих методов обнаружения атак:

Ответ: способность выявлять аномалии в поведении пользователей

13. Роль нейронных сетей в обнаружении атак:

Ответ: нейронные сети могут эффективно выявлять как аномалии, так и злоупотребления, обеспечивая гибкость и адаптивность в анализе данных

14. Нульевой день (zero-day) уязвимость это:

Ответ: это уязвимость, о которой еще не известно разработчикам программного обеспечения, и которая активно используется злоумышленниками

15. Мониторинг сетевого трафика в IDS включает:

Ответ: анализ пакетов данных, выявление подозрительной активности и оценку уровня серьезности атаки

16. Этапы анализа инцидентов безопасности:

Ответ: сбор данных, анализ инцидента, идентификация уязвимостей, оценка ущерба и разработка рекомендаций по предотвращению будущих атак

17. Гибридные методы" обнаружения атак это:

Ответ: гибридные методы сочетают преимущества различных подходов, таких как анализ поведения и сигнатурный анализ, для повышения точности обнаружения

18. Преднамеренное действие, направленное на нарушение работы компьютерной системы или сети, получение несанкционированного доступа к данным или их уничтожение:

Ответ: компьютерная атака

19. Целями использования вирусов в компьютерных атаках являются:

Ответ: локальные и удаленные

20. Компьютерные атаки по способу их выполнения бывают:

Ответ: компьютерная атака

21. Поисковые мероприятия проводятся в местах:

Ответ: где возможна утечка конфиденциальной информации (переговорные, кабинеты руководства, автомобили)

22. Поисковые мероприятия могут быть:

Ответ: внеплановые и периодические

Тестовые задания закрытого типа (2 семестр):

23. Наиболее безопасный метод аутентификации**:**

1. Пароль
2. Двухфакторная аутентификация
3. Ответ на секретный вопрос
4. **Биометрическая аутентификация**

24. Бэкдор в контексте компьютерной безопасности это:

1. Легитимный доступ к системе
2**. Уязвимость, позволяющая злоумышленнику получить доступ к системе без авторизации**
3. Программа для защиты от вирусов
4. Метод шифрования данных

25. Социальная инженерия это:

1. **Манипуляция людьми для получения конфиденциальной информации или доступа к системам**
2. Использование технических средств для защиты информации
3. Процесс анализа сетевого трафика
4. Метод шифрования данных

26. Методы для защиты от атак типа "отказ в обслуживании" (DoS):

1. Использование антивирусного ПО
3. **Настройка брандмауэра и фильтраци трафика**

2. Регулярные обновления программного обеспечения

4. Обучение сотрудников

27. Протоколов, используемый для безопасной передачи данных по сети:

1. HTTP

3. FTP

2. **HTTPS**

4. SMTP

28. Метод, используемый для защиты от SQL-инъекций:

1. Использование сложных паролей

3. **Параметризованные запросы**

2. Регулярные обновления системы

4. Шифрование данных

29: Тип атак, использующий множество зараженных устройств для выполнения атаки:

1. **DDos - атака**

3. Фишинг

2. SQL-инъекция

4. Вредоносное ПО

30: План реагирования на инциденты это:

1. **Документ, описывающий действия при возникновении инцидента безопасности**

3. Процесс шифрования данных

2. Метод защиты данных

4. Программа для анализа трафика

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

КУРСОВОЙ ПРОЕКТ

Основная цель курсового проекта по дисциплине «Теория анализа компьютерных атак» заключается в приобретении студентами навыков анализа компьютерных атак на объектах обработки конфиденциальной информации, рациональному подбору методик и способов оценки компьютерных атак, рисков для эффективного функционирования информационных систем и систем защиты информации.

При выполнении курсового проекта, кроме конспекта лекций по дисциплине «Теория анализа компьютерных атак», рекомендуется использовать дополнительную литературу, приведенную в библиографическом списке.

Курсовой проект состоит из трех частей. В первой части студенту необходимо выбрать и описать объект исследования (информационную систему) привести ее структурную схему, схему СВС, состав средств информатизации и защиты. Указать вид деятельности отдела предприятия, топологию сети и количество рабочих мест.

Во второй части проекта для выбранной информационной системы проводится анализ актуальных угроз, уязвимостей и каналов несанкционированного доступа и утечки информации. Осуществляется обзор нормативно-правовой базы по данному вопросу и подбор необходимых средств защиты для повышения уровня защищённости организации.

В третьей части проводится анализ рисков безопасности различными методами и осуществляется оценка эффективности предложенных решений, с целью управления рисками и снижению их.

Оформление проекта

Курсовая проект выполняется на листах формата А4 с соблюдением требований стандарта университета на оформление расчётно-графических работ. Объем пояснительной записки не менее 15 страниц машинописного текста: предпочтительный шрифт Times New Roman; размер шрифта 13; междустрочный интервал 1,5; выравнивание по ширине.

Пояснительная записка должна содержать:

1. титульный лист, оформленный по стандарту и задание на курсовой проект;
2. первую часть, в которой приводится описание информационной системы, топологии и характеристики ЛС в соответствии со стандартами, необходимое оборудование для ее функционирования, структурная схема ИС;

3. вторую часть, в которой приводится список актуальных угроз уязвимостей и каналов НСД, приводится анализ нормативно-правовой базы по типу ИС и системы защиты информации; приводится список предложений по управлению рисками и повышению уровня защищенности ИС.
4. третью часть, где приводится анализ рисков и анализ эффективности предложенных решений;
5. список использованных литературных и Интернет-источников.

ВОПРОСЫ К ЗАЩИТЕ КУРСОВОГО ПРОЕКТА

1. Основы теории рисков.
2. Состав элементов КОИБАС (организационный, криптографический, правовой, программно-аппаратный, инженерно-технический элементы).
3. Подробно осветить начальные этапы формирования процесса оценки рисков. Формирование дерева уязвимостей. Формализация оценки рисков.
4. Построение графа компрометации. Указать типы вершин, типы рёбер. Способы формальных вычислений.
5. Использование графа атаки. Расчёты экономических показателей с использованием графа атаки. Оптимизация набора механизмов безопасности с использованием графа атаки.
6. Оптимизация состава КОИБАС на основе модели Клеменса-Хоффмана.
7. Теория уровней (зональная модель) при расчете уязвимости информации.
8. Приложение теории надежности к оценке защищенности ИС.
9. Определение уровня защищенности.
10. Особенности определения угроз при построении КОИБАС
11. Определение стоимость потерь.
12. Определение уровня защищённости системы с учётом угроз, рисков и производительности.
13. Основы аудита.
14. Особенности применения табличных способов оценки рисков
15. Оценка рисков системы по методу Digital Security (лабораторная работа).
16. Методы определения эффективности компьютерных атак
17. Особенности определения видов нарушителей.
18. Особенности подбора средств защиты.

4 СВЕДЕНИЯ О ФОНДЕ ОЦЕНОЧНЫХ СРЕДСТВ И ЕГО СОГЛАСОВАНИИ

Фонд оценочных средств для аттестации по дисциплине «**Теория анализа компьютерных атак**» представляет собой компонент основной профессиональной образовательной программы специалитета по специальности **10.05.03 Информационная безопасность автоматизированных систем** (Специализация "Безопасность открытых информационных систем").

Старший преподаватель кафедры информационной безопасности: А.А. Бабаева.

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

Председатель методической комиссии  О.С. Витренко