МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Чувашский государственный университет имени И. Н. Ульянова»
(ФГБОУ ВО «ЧГУ им. И.Н. Ульянова»)

Факультет информатики и вычислительной техники

Кафедра компьютерных технологий

Утверждено
на заседании кафедры компьютерных технологий
Заведующий кафедрой Т. А. Лавина

___ _____25.03.2022

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
(ФОНД ОЦЕНОЧНЫХ СРЕДСТВ)

«Информационная безопасность в профессиональной деятельности»

Направление подготовки / специальность 09.04.03 Прикладная информатика

Квалификация выпускника Магистр

Направленность (профиль) / специализация « Искусственный интеллект и бизнес-аналитика»

Год начала подготовки - 2022

Чебоксары - 2022

Составитель(и):
Доцент, кандидат технических наук Ванюлин А.Н.

Согласовано
методической комиссией факультета информатики и вычислительной техники 25.03.2022, протокол № 8

Декан факультета А. В. Щипцова

Паспорт

оценочных материалов для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине (модулю)

Информационная безопасность в профессиональной деятельности

Перечень оценочных материалов и индикаторов достижения компетенций, сформированность которых они контролируют

Наименование оценочного средства	Коды индикаторов достижения формируемых компетенции	Номер приложения
Тест	ИД-1 $_{ПК-8}$ ИД-2 $_{ПК-8}$	1
Реферат (эссе, доклад)	ИД-1 $_{ПК-8}$ ИД-2 $_{ПК-8}$	2
Зачет	ИД-1 $_{ПК-8}$ ИД-2 $_{ПК-8}$	3

Разработали: _____ А.А. Филиппов

_____ С.О. Иванов

Утверждено на заседании кафедры «Информационные системы»
протокол № 3 от «11» октября 2021 года
Заведующий кафедрой _____ А.А. Романов

I. Текущий контроль

Приложение 1

Тесты

1. Процедура проведения тестирования

Количество проводимых тестов в течение всего периода освоения дисциплины	1 тест
Общее количество тестовых вопросов в банке тестов	30 вопросов
Количество задаваемых тестовых вопросов в одном тесте	10 вопросов
Формат проведения тестирования	Письменный / Электронный
Сроки / Периодичность проведения тестирования	в конце семестра

2. Шкала оценивания с учетом срока сдачи

Количество правильных ответов / Процент правильных ответов	Балл
Более 75%	Отлично
55-75%	Хорошо
40-55%	Удовлетворительно
Менее 40%	Неудовлетворительно

3. Тестовые задания

Правильные ответы выделены жирным.

1) К правовым методам, обеспечивающим информационную безопасность, относятся:
- Разработка аппаратных средств обеспечения правовых данных
- Разработка и установка во всех компьютерных правовых сетях журналов учета действий
- Разработка и конкретизация правовых нормативных актов обеспечения безопасности

2) Основными источниками угроз информационной безопасности являются все указанное в списке:
- Хищение жестких дисков, подключение к сети, инсайдерство
- Перехват данных, хищение данных, изменение архитектуры системы
- Хищение данных, подкуп системных администраторов, нарушение регламента работы

3) Виды информационной безопасности:
- Персональная, корпоративная, государственная
- Клиентская, серверная, сетевая
- Локальная, глобальная, смешанная

4) Цели информационной безопасности – своевременное обнаружение, предупреждение:
- несанкционированного доступа, воздействия в сети
- инсайдерства в организации
- чрезвычайных ситуаций

5) Основные объекты информационной безопасности:
- Компьютерные сети, базы данных
- Информационные системы, психологическое состояние пользователей
- Бизнес-ориентированные, коммерческие системы

6) Основными рисками информационной безопасности являются:
- Искажение, уменьшение объема, перекодировка информации
- Техническое вмешательство, выведение из строя оборудования сети
- Потеря, искажение, утечка информации

7) К основным принципам обеспечения информационной безопасности относится:
- Экономической эффективности системы безопасности
- Многоплатформенной реализации системы
- Усиления защищенности всех звеньев системы

8) Основными субъектами информационной безопасности являются:
- руководители, менеджеры, администраторы компаний
- органы права, государства, бизнеса
- сетевые базы данных, фаерволлы

9) К основным функциям системы безопасности можно отнести все перечисленное:
- Установление регламента, аудит системы, выявление рисков
- Установка новых офисных приложений, смена хостинг-компании
- Внедрение аутентификации, проверки контактных данных пользователей

10) Принципом информационной безопасности является принцип недопущения:
- Неоправданных ограничений при работе в сети (системе)
- Рисков безопасности сети, системы
- Презумпции секретности

11) Принципом политики информационной безопасности является принцип:
- Невозможности миновать защитные средства сети (системы)
- Усиления основного звена сети, системы
- Полного блокирования доступа при риск-ситуациях

12) Принципом политики информационной безопасности является принцип:
- Усиления защищенности самого незащищенного звена сети (системы)
- Перехода в безопасное состояние работы сети, системы
- Полного доступа пользователей ко всем ресурсам сети, системы

13) Принципом политики информационной безопасности является принцип:
- Разделения доступа (обязанностей, привилегий) клиентам сети (системы)
- Одноуровневой защиты сети, системы
- Совместимых, однотипных программно-технических средств сети, системы

14) К основным типам средств воздействия на компьютерную сеть относится:
- Компьютерный сбой
- Логические закладки («мины»)
- Аварийное отключение питания

15) Когда получен спам по e-mail с приложенным файлом, следует:
- Прочитать приложение, если оно не содержит ничего ценного – удалить
- Сохранить приложение в парке «Спам», выяснить затем IP-адрес генератора спама
- Удалить письмо с приложением, не раскрывая (не читая) его

16) Принцип Кирхгофа:
- Секретность ключа определена секретностью открытого сообщения
- Секретность информации определена скоростью передачи данных
- Секретность закрытого сообщения определяется секретностью ключа

17) ЭЦП – это:
- Электронно-цифровой преобразователь
- Электронно-цифровая подпись
- Электронно-цифровой процессор

18) Наиболее распространены угрозы информационной безопасности корпоративной системы:
- Покупка нелицензионного ПО

- Ошибки эксплуатации и неумышленного изменения режима работы системы
- Сознательного внедрения сетевых вирусов

19) Наиболее распространены угрозы информационной безопасности сети:
- Распределенный доступ клиент, отказ оборудования
- Моральный износ сети, инсайдерство
- Сбой (отказ) оборудования, нелегальное копирование данных

20) Наиболее распространены средства воздействия на сеть офиса:
- Слабый трафик, информационный обман, вирусы в интернет
- Вирусы в сети, логические мины (закладки), информационный перехват
- Компьютерные сбои, изменение администрирования, топологии

21) Утечкой информации в системе называется ситуация, характеризуемая:
- Потерей данных в системе
- Изменением формы информации
- Изменением содержания информации

22) Свойствами информации, наиболее актуальными при обеспечении информационной безопасности являются:
- Целостность
- Доступность
- Актуальностьl

23) Угроза информационной системе (компьютерной сети) – это:
- Вероятное событие
- Детерминированное (всегда определенное) событие
- Событие, происходящее периодически

24) Информация, которую следует защищать (по нормативам, правилам сети, системы) называется:
- Регламентированной
- Правовой
- Защищаемой

25) Разновидностями угроз безопасности (сети, системы) являются все перчисленное в списке:
- Программные, технические, организационные, технологические
- Серверные, клиентские, спутниковые, наземные
- Личные, корпоративные, социальные, национальные

26) Окончательно, ответственность за защищенность данных в компьютерной сети несет:
- Владелец сети
- Администратор сети
- Пользователь сети

27) Политика безопасности в системе (сети) – это комплекс:
- Руководств, требований обеспечения необходимого уровня безопасности
- Инструкций, алгоритмов поведения пользователя в сети
- Нормы информационного права, соблюдаемые в сети

28) Наиболее важным при реализации защитных мер политики безопасности является:
- Аудит, анализ затрат на проведение защитных мер
- Аудит, анализ безопасности
- Аудит, анализ уязвимостей, риск-ситуаций

29) Антивирус, который обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:
- детектор
- доктор
- сканер
- ревизор
- сторож

30) Потенциальные угрозы, против которых направлены технические меры защиты информации

- Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей

- Потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения

- Потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками.

- Потери информации из-за не достаточной установки сигнализации в помещении.

- Процессы преобразования, при котором информация удаляется

Приложение 2

Реферат (эссе, доклад)

1. Процедура проведения

Общее количество тем	19 тем
Сроки / Периодичность выдачи и контроля решения задач	в течение семестра

2. Шкала оценивания с учетом срока сдачи

Критерии оценки качества решения задачи	Балл
Обучающийся показывает высокий уровень знаний в области темы подготовленного реферата. Тема реферата актуальна, проблематика вопросов раскрыта. Используются современные инструменты передачи информации	Отлично
Обучающийся показывает достаточный уровень знаний в области темы подготовленного реферата. Тема реферата актуальна, проблематика вопросов раскрыта. Используются современные инструменты передачи информации	Хорошо
Обучающийся показывает недостаточный уровень знаний по теме научного исследования. Тема реферата актуальна, но проблематика вопросов раскрыта слабо. Слабо используются современные инструменты передачи информации	Удовлетворительно
Обучающийся показывает низкий уровень знаний в области научного исследования. Тема реферата актуальна, но проблематика вопросов не раскрыта. Не используются современные инструменты передачи информации	Неудовлетворительно

3. Темы
4. Принципы и правила управления персоналом
5. Принципы и правила организации службы безопасности
6. Средства физической безопасности
7. Техническая защита информации. Каналы утечек
8. Системы управления идентификационными данными и доступом (IAM);
9. Системы однократной и многофакторной аутентификации в корпоративных сетях;
10. Системы управления доступом к информации (IRM);
11. Системы защиты от атак на прикладном уровне (WAF);
12. Системы управления инцидентами и событиями ИБ (SIEM);
13. Системы защиты от утечки конфиденциальной информации (DLP);
14. Объекты политики безопасности ОС, примеры реализации
15. Средства шифрования файлов, дисков, архивов
16. Средства управления целостностью данных
17. Система обнаружения атак(IDS)
18. Поиск уязвимостей
19. Системы управления соответствием требованиям ИБ (Compliance Management);

II. Промежуточная аттестация

Приложение 3

Зачет

1. Процедура проведения

Общее количество вопросов к зачету	20 вопросов
Количество основных задаваемых вопросов	5 вопросов
Формат проведения	Устно

2. Шкала оценивания с учетом текущего контроля работы обучающегося в семестре

Критерии оценки уровня сформированности компетенций по дисциплине	Балл
выставляется обучающемуся выполнившему тест и защитившему реферат, чей уровень знаний, умений и навыков соответствует уровню оценок «отлично», «хорошо» или «удовлетворительно».	Зачтено
выставляется обучающемуся, не выполнившему тест и не защитившему реферат в течение семестра, либо чей уровень знаний, умений и навыков соответствует уровню оценки «неудовлетворительно».	Не зачтено

3. Вопросы и задачи (при необходимости) к зачету

1. Чем угроза ИБ отличается от уязвимости ИБ?
2. Дайте определение понятию риска.
3. Какие недостатки имеют несимметричные методы шифрования перед симметричными?
4. В чем заключается проблема управления ключами?
5. Где используется стеганография?
6. Опишите принцип работы цифровой подписи документа.
7. Что такое государственная тайна и каков ответственность за ее несоблюдение?
8. Какие документы регламентируют защиту персональных данных.
9. Как охраняются результаты интеллектуальной деятельности?
10. Какая существует ответственность за нарушения в сфере информационной безопасности?
11. Какие существуют способы оценки ИБ.
12. Какую роль играют организационно-режимные меры в сфере ИБ?
13. Дайте определение понятию политика безопасности.
14. В чем сущность атаки «Квид про кво».
15. Что такое «фишинг», «вишинг», «смишинг», «фарминг»?
16. Как защитить от мошенников в Интернете?

17. Назовите основные угрозы физической безопасности.
18. Назовите программные средства для контроля периметра.
19. Опишите принципы работы антивирусов?
20. Какие существуют виды сетевых экранов?