Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Богдалова Елена Вячеславовна
Должность: Проректор по образовательной деятельности
Дата подписания: 07.08.2025 12:55:11
Уникальный программный ключ:
ec85dd5a839619d48ea76b2d23dba88a9c82071a

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное образовательное учреждение инклюзивного высшего образования
«Российский государственный университет социальных технологий»
(ФГБОУ ИВО «РГУ СоцТех»)

УТВЕРЖДАЮ

Проректор по образовательной деятельности

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

Б1.О.22 Защита компьютеров и сетей
наименование дисциплины

01.03.02 «Прикладная математика и информатика»
шифр и наименование направления подготовки

Вычислительная математика и информационные технологии
направленность (профиль)

Москва 2024

Содержание

1. Паспорт фонда оценочных средств……..
2. Перечень оценочных средств……
3. Описание показателей и критериев оценивания компетенций……
4. Методические материалы, определяющие процедуры оценивания результатов обучения, характеризующих этапы формирования компетенций…….
5. Материалы для проведения текущего контроля и промежуточной аттестации……

1. ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине «Защита компьютеров и сетей»

Оценочные средства составляются в соответствии с рабочей программой дисциплины и представляют собой совокупность контрольно-измерительных материалов (типовые задачи (задания), контрольные работы, тесты и др.), предназначенных для измерения уровня достижения обучающимися установленных результатов обучения.

Оценочные средства используются при проведении текущего контроля успеваемости и промежуточной аттестации.

Таблица 1 - Перечень компетенций, формируемых в процессе освоения дисциплины

Код компетенции	**Наименование результата обучения**
ОПК-4	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

Конечными результатами освоения дисциплины являются сформированные когнитивные дескрипторы «знать», «уметь», «владеть», расписанные по отдельным компетенциям. Формирование дескрипторов происходит в течение всего семестра по этапам в рамках контактной работы, включающей различные виды занятий и самостоятельной работы, с применением различных форм и методов обучения.

2. ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ[1]

Таблица 2

№	Наименование оценочного средства	Характеристика оценочного средства	Представление оценочного средства в ФОС
1	Устный опрос	Средство контроля усвоения учебного материала темы, раздела или разделов дисциплины, организованное как учебное занятие в виде собеседования преподавателя с обучающимися.	Вопросы по темам/разделам дисциплины
2	Тест	Средство, позволяющее оценить уровень знаний обучающегося путем выбора им одного из нескольких вариантов ответов на поставленный вопрос. Возможно использование тестовых вопросов, предусматривающих ввод обучающимся короткого и однозначного ответа на поставленный вопрос.	Тестовые задания
3	Контрольная работа, защита отчетов по практическим работам	Различают задачи и задания: а) репродуктивного уровня, позволяющие оценивать и диагностировать знание фактического материала (базовые понятия, алгоритмы, факты) и умение правильно использовать специальные термины и понятия, узнавание объектов изучения в рамках определенного раздела дисциплины; б) реконструктивного уровня, позволяющие оценивать и диагностировать умения синтезировать, анализировать, обобщать фактический и теоретический материал с формулированием конкретных выводов, установлением причинно-следственных связей; в) творческого уровня, позволяющие оценивать и диагностировать умения, интегрировать знания различных областей, аргументировать собственную точку зрения.	Комплект разноуровневых задач (заданий)

[1] Указываются оценочные средства, применяемые в ходе реализации рабочей программы данной дисциплины.

3. ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ КОМПЕТЕНЦИЙ

Оценивание результатов обучения по дисциплине «Защита компьютеров и сетей» осуществляется в соответствии с Положением о текущем контроле успеваемости и промежуточной аттестации обучающихся.

Предусмотрены следующие виды контроля: текущий контроль (осуществление контроля всех видов аудиторной и внеаудиторной деятельности обучающегося с целью получения первичной информации о ходе усвоения отдельных элементов содержания дисциплины) и промежуточная аттестация (оценивается уровень и качество подготовки по дисциплине в целом).

Показатели и критерии оценивания компетенций, формируемых в процессе освоения данной дисциплины, описаны в табл. 3.

Таблица 3.

Код компетенции	Уровень освоения компетенции	Индикаторы достижения компетенции	Вид учебных занятий[2], работы, формы и методы обучения, способствующие формированию и развитию компетенций[3]	Контролируемые разделы и темы дисциплины[4]	Оценочные средства, используемые для оценки уровня сформированности компетенции[5]	Критерии оценивания результатов обучения
ОПК-4	Знает					
	Недостаточный уровень Оценка «незачтено», «неудовлетворительно»	*ОПК-4.4-1.* Знает: принципы, работы современных информационных технологий и возможности их использования для решения задач профессиональной деятельности.	Лекционные и практические занятия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	Текущий контроль – устный опрос, контрольная работа, тестирование, защита отчетов по практическим работам	Не знает значительной части материала курса, не способен самостоятельно выделять главные положения в изученном материале дисциплины
	Базовый уровень Оценка, «зачтено», «удовлетворительно»	*ОПК-4.4-1.* Знает: принципы, работы современных информационных технологий и возможности их использования для решения задач	Лекционные и практические занятия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление	Текущий контроль – устный опрос, контрольная работа, тестирование, защита отчетов по практическим работам	Знает не менее 50 % основного материала курса, однако испытывает затруднения в его применении

[2] Лекционные занятия, практические занятия, лабораторные занятия, самостоятельная работа…

[3] Необходимо указать активные и интерактивные методы обучения (например, интерактивная лекция, работа в малых группах, методы мозгового штурма и т.д.), способствующие развитию у обучающихся навыков командной работы, межличностной коммуникации, принятия решений, лидерских качеств.

[4] Наименование темы (раздела) берется из рабочей программы дисциплины.

[5] Оценочное средство должно выбираться с учетом запланированных результатов освоения дисциплины, например:
«Знать» – собеседование, коллоквиум, тест…
«Уметь», «Владеть» – индивидуальный или групповой проект, кейс-задача, деловая (ролевая) игра, портфолио…

		профессиональной деятельности.		безопасностью.		
	Средний уровень Оценка «зачтено», «хорошо»	*ОПК-4.4-1.* Знает: принципы, работы современных информационных технологий и возможности их использования для решения задач профессиональной деятельности.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	Текущий контроль – устный опрос, контрольная работа, тестирование, защита отчетов по практическим работам	Знает основную часть материала курса, способен применить изученный материал на практике, испытывает незначительные затруднения в решении задач
	Высокий уровень Оценка «зачтено», «отлично»	*ОПК-4.4-1.* Знает: принципы, работы современных информационных технологий и возможности их использования для решения задач профессиональной деятельности.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	Текущий контроль – устный опрос, контрольная работа, тестирование, защита отчетов по практическим работам	Показывает глубокое знание и понимание материала, способен применить изученный материал на практике
	Умеет					
	Недостаточный уровень Оценка «незачтено», «неудовлетворительно»	*ОПК-4.4-2.* Умеет: использовать принципы работы современных информационны	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных	Текущий контроль – устный опрос, контрольная работа, тестирование, защита отчетов по практическим работам	Не знает значительной части материала курса, не способен самостоятельно выделять главные положения в изученном материале дисциплины

		х технологий и применяет их для решения задач профессиональной деятельности.	и сдача промежуточной аттестации, подготовка и сдача зачета	систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.		
	Базовый уровень Оценка, «зачтено», «удовлетворительно»	*ОПК-4.4-2.* Умеет: использовать принципы работы современных информационных технологий и применяет их для решения задач профессиональной деятельности.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	6. Введение в информационную безопасность (ИБ). 7. Технологии защиты данных. 8. Технологии защиты вычислительных систем. 9. Технологии обнаружения вторжений. 10. Управление безопасностью.	Текущий контроль – устный опрос, контрольная работа, тестирование, защита отчетов по практическим работам	Умеет воспроизвести не менее 50 % основного материала курса, однако испытывает затруднения при решении практических задач
	Средний уровень Оценка «зачтено», «хорошо»	*ОПК-4.4-2.* Умеет: использовать принципы работы современных информационных технологий и применяет их для решения задач профессиональной деятельности.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	Текущий контроль – устный опрос, контрольная работа, тестирование, защита отчетов по практическим работам	Умеет решать стандартные профессиональные задачи с применением полученных знаний, испытывает незначительные затруднения в решении задач
	Высокий уровень Оценка «зачтено»,	*ОПК-4.4-2.* Умеет: использовать принципы	Лекционные и практические занятия, работа в малых группах, интерактивная лекция,	1. Введение в информационную безопасность (ИБ). 2. Технологии	Текущий контроль – устный опрос, контрольная работа, тестирование, защита	Умеет решать стандартные профессиональные задачи с применением

	«отлично»	работы современных информационных технологий и применяет их для решения задач профессиональной деятельности.	дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	отчетов по практическим работам	полученных знаний, показывает глубокое знание и понимание материала, способен решить задачу при изменении формулировки
	Владеет					
	Недостаточный уровень Оценка «незачтено», «неудовлетворительно»	*ОПК-4.4-3.* Владеет: навыками работы современных информационных технологий для решения задач профессиональной деятельности.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	Текущий контроль – устный опрос, контрольная работа, тестирование, защита отчетов по практическим работам	Не знает значительной части материала курса, не способен самостоятельно выделять главные положения в изученном материале дисциплины
	Базовый уровень Оценка, «зачтено», «удовлетворительно»	*ОПК-4.4-3.* Владеет: навыками работы современных информационных технологий для решения задач профессиональной деятельности.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	6. Введение в информационную безопасность (ИБ). 7. Технологии защиты данных. 8. Технологии защиты вычислительных систем. 9. Технологии обнаружения вторжений. 10. Управление безопасностью.	Текущий контроль – устный опрос, контрольная работа, тестирование, защита отчетов по практическим работам	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, усвоил основное содержание материала дисциплины, но имеет пробелы в усвоении материала. Имеет несистематизированные знания основных разделов дисциплины.

	Средний уровень Оценка «зачтено», «хорошо»	*ОПК-4.4-3.* Владеет: навыками работы современных информационных технологий для решения задач профессиональной деятельности.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	Текущий контроль – устный опрос, контрольная работа, тестирование, защита отчетов по практическим работам	Владеет навыками теоретического и экспериментального исследования объектов профессиональной деятельности, способен самостоятельно выделять главные положения в изученном материале. Испытывает незначительные затруднения в решении задач.
	Высокий уровень Оценка «зачтено», «отлично»	*ОПК-4.4-3.* Владеет: навыками работы современных информационных технологий для решения задач профессиональной деятельности.	Лекционные и практические занятия, работа в малых группах, интерактивная лекция, дискуссия, самостоятельная работа обучающихся, подготовка и сдача промежуточной аттестации, подготовка и сдача зачета	1. Введение в информационную безопасность (ИБ). 2. Технологии защиты данных. 3. Технологии защиты вычислительных систем. 4. Технологии обнаружения вторжений. 5. Управление безопасностью.	Текущий контроль – устный опрос, контрольная работа, тестирование, защита отчетов по практическим работам	Свободно владеет навыками теоретического и экспериментального исследования, показывает глубокое знание и понимание изученного материала

4. Методические материалы, определяющие процедуры оценивания результатов обучения

Задания в форме устного опроса:

Устный опрос используется для текущего контроля успеваемости обучающихся по дисциплине в качестве проверки результатов освоения материала. Каждому студенту выдается свой собственный, узко сформулированный вопрос. Ответ должен быть четким и кратким, содержащим все основные характеристики описываемого понятия. В своем ответе студент должен показать умения прослеживать причинно-следственные связи и навыки рассуждений и доказательства.

Задания в форме практических работ. Комплект разноуровневых задач (заданий)

Практическая работа представляет собой контрольное мероприятие по учебному материалу каждой темы (раздела) дисциплины, состоящее в индивидуальном выполнении обучающимся практических заданий для оценки полученных знаний, умений и владений компетенциями, формируемыми по данной дисциплине.

Выполнение практических работ является средством текущего контроля успеваемости обучающихся по дисциплине и может включать в себя следующие типы заданий: задания типового вида и задания творческого характера, по результатам выполнения практических заданий обучающие оформляют отчеты, содержащие анализ полученных результатов и выводы.

Тестовые задания. Задания в форме тестирования

Тест представляет собой контрольное мероприятие по учебному материалу каждой темы (раздела) дисциплины, состоящее в выполнении обучающимся системы стандартизированных заданий, которая позволяет автоматизировать процедуру измерения уровня знаний и умений обучающегося.

Тестирование является средством текущего контроля успеваемости обучающихся по дисциплине и может включать в себя следующие типы заданий: задание с единственным выбором ответа из предложенных вариантов, задание на определение верных и неверных суждений; задание с множественным выбором ответов.

В каждом задании необходимо выбрать все правильные ответы.

5. Материалы для проведения текущего контроля и промежуточной аттестации

Задания в форме устного опроса

5 семестр

1. Введение в информационную безопасность (ИБ)
2. Основные понятия ИБ.
3. Анализ угроз.
4. Проблемы безопасности компьютерных сетей.
5. Политика безопасности.
6. Основные составляющие политики безопасности.
7. Нормативно-правовое обеспечение ИБ.
8. Стандарты ИБ.
9. Международные стандарты в сфере ИБ.
10. Принципы защиты информационных систем (ИС).
11. Технологии защиты данных.
12. Принципы криптозащиты.
13. Криптографические алгоритмы.
14. Криптоанализ.
15. Симметричные и асимметричные системы шифрования.
16. Технологии электронно-цифровой подписи.
17. Функции хэширования.
18. Технологии аутентификации.
19. Биометрическая аутентификация.

6 семестр

1. Технологии защиты вычислительных систем.
2. Обеспечение безопасности операционных систем (ОС).
3. Межсетевые экраны.
4. Сертификация и стандартизация.
5. Защита в виртуальных сетях VPN.
6. Защита на уровнях модели OSI.
7. Технологии обнаружения вторжений.
8. Средство анализа сетевого трафика Wireshark.
9. Сканирование сети.
10. Анализ защищенности.
11. Обнаружение атак.
12. Программные средства обнаружения вторжения.
13. Защита удаленного доступа.
14. Защита от вирусов и спама.
15. Управление безопасностью.
16. Задачи управления ИБ в информационных системах (ИС).
17. Архитектура и функционирование систем управления ИБ в (ИС).
18. Аудит и мониторинг безопасности (ИС).
19. Обзор систем управления безопасностью.

Тестовые задания

5 семестр

1. Кто является основным ответственным за определение уровня классификации информации?

a) Руководитель среднего звена
b) Высшее руководство
c) Владелец
d) Пользователь

2. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

a) Сотрудники
b) Хакеры
c) Атакующие
d) Контрагенты (лица, работающие по договору)

3. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

a) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
b) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
c) Улучшить контроль за безопасностью этой информации
d) Снизить уровень классификации этой информации

4. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?

a) Поддержка высшего руководства
b) Эффективные защитные меры и методы их внедрения
c) Актуальные и адекватные политики и процедуры безопасности
d) Проведение тренингов по безопасности для всех сотрудников

5. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

a) Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
b) Когда риски не могут быть приняты во внимание по политическим соображениям
c) Когда необходимые защитные меры слишком сложны
d) Когда стоимость контрмер превышает ценность актива и потенциальные потери

6. Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?

a) Только военные имеют настоящую безопасность
b) Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности
c) Военным требуется больший уровень безопасности, т.к. их риски существенно выше
d) Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности

7. Защита информации от утечки – это деятельность по предотвращению:

a) получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации;

b) воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации;

c) воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений;

d) неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа;

e) несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации.

8. Защита информации это:

a) процесс сбора, накопления, обработки, хранения, распределения и поиска информации;

b) преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа;

c) получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств;

d) совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям;

e) деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё.

9. Естественные угрозы безопасности информации вызваны:

a) деятельностью человека;

b) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

c) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

d) корыстными устремлениями злоумышленников;

e) ошибками при действиях персонала.

10. Искусственные угрозы безопасности информации вызваны:

a) деятельностью человека;

b) ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения;

c) воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека;

d) корыстными устремлениями злоумышленников;

e) ошибками при действиях персонала.

11. К основным непреднамеренным искусственным угрозам АСОИ относится:

a) физическое разрушение системы путем взрыва, поджога и т.п.;

b) перехват побочных электромагнитных, акустических и других излучений устройств и линий связи;

c) изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.;

d) чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств;

e) неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы.

12. К посторонним лицам нарушителям информационной безопасности относится:

a) представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации;

b) персонал, обслуживающий технические средства;

c) технический персонал, обслуживающий здание;

d) пользователи;

e) сотрудники службы безопасности.

f) представители конкурирующих организаций.

g) лица, нарушившие пропускной режим;

13. Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:

a) черный пиар;

b) фишинг;

c) нигерийские письма;

d) источник слухов;

e) пустые письма.

14. Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:

a) черный пиар;

b) фишинг;

c) нигерийские письма;

d) источник слухов;

e) пустые письма.

15. Активный перехват информации - это перехват, который:

a) заключается в установке подслушивающего устройства в аппаратуру средств обработки информации;

b) основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций;

c) неправомерно использует технологические отходы информационного процесса;

d) осуществляется путем использования оптической техники;

e) осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера.

16. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется:

a) активный перехват;

b) пассивный перехват;

c) аудиоперехват;

d) видеоперехват;

e) просмотр мусора.

17. Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:

a) активный перехват;
b) пассивный перехват;
c) аудиоперехват;
d) видеоперехват;
e) просмотр мусора.

18. Перехват, который осуществляется путем использования оптической техники называется:

a) активный перехват;
b) пассивный перехват;
c) аудиоперехват;
d) видеоперехват;
e) просмотр мусора.

19. Степень защищенности информации от негативного воздействия на неё с точки зрения нарушения её физической и логической целостности или несанкционированного использования — это

a) уязвимость информации
b) надежность информации
c) защищенность информации
d) безопасность информации

20. Проверка подлинности субъекта по предъявленному им идентификатору для принятия решения о предоставлении ему доступа к ресурсам системы — это

a) аудит
b) аутентификация
c) авторизация
d) идентификация

21. Совокупность свойств, обусловливающих пригодность информации удовлетворять определенные потребности в соответствии с ее назначением, называется

a) актуальностью информации
b) доступностью
c) качеством информации
d) целостностью

22. Первым этапом разработки системы защиты ИС является

a) анализ потенциально возможных угроз информации
b) изучение информационных потоков
c) стандартизация программного обеспечения
d) оценка возможных потерь

23. Надежность системы защиты информации определяется

a) усредненным показателем
b) самым слабым звеном
c) количеством отраженных атак
d) самым сильным звеном

24. Политика информационной безопасности — это
a) профиль защиты
b) итоговый документ анализа рисков
c) стандарт безопасности
d) совокупность законов, правил, определяющих управленческие и проектные решения в области защиты информации

25. Присвоение субъектам и объектам доступа уникального номера, шифра, кода и т.п. с целью получения доступа к информации — это
a) аутентификация
b) идентификация
c) аудит
d) авторизация

26. Какой тип воздействия осуществляет программная закладка, которая внедряется в ПЗУ, системное или прикладное программное обеспечение и сохраняет всю или выбранную информацию в скрытой области памяти:
a) компрометация
b) перехват
c) наблюдение
d) уборка мусора

27. Содержанием параметра угрозы безопасности информации «конфиденциальность» является
a) несанкционированная модификация
b) искажение
c) несанкционированное получение
d) уничтожение

28. Требования к техническому обеспечению системы защиты:
a) аппаратурные и физические
b) управленческие и документарные
c) процедурные и раздельные
d) административные и аппаратурные

29. Цель процесса внедрения и тестирования средств защиты —
a) определить уровень расходов на систему защиты
b) выявить нарушителя
c) гарантировать правильность реализации средств защиты
d) выбор мер и средств защиты

30. Возможность получения необходимых пользователю данных или сервисов за разумное время характеризует свойство
a) восстанавливаемость
b) детермированность
c) целостность
d) доступность

31. Трояские программы — это
a) программы-вирусы, которые распространяются самостоятельно
b) все программы, содержащие ошибки

c) часть программы с известными пользователю функциями, способная выполнять действия с целью причинения определенного ущерба
d) текстовые файлы, распространяемые по сети

32. Наиболее надежным механизмом для защиты содержания сообщений является
a) специальный аппаратный модуль
b) специальный режим передачи сообщения
c) дополнительный хост
d) криптография

33. Основной целью системы брандмауэра является управление доступом
a) к архивам
b) внутри защищаемой сети
c) к секретной информации
d) к защищаемой сети

34. Процесс имитации хакером дружественного адреса называется
a) «крэком»
b) проникновением
c) взломом
d) «спуфингом»

35. Предоставление легальным пользователем дифференцированных прав доступа к ресурсам системы — это
a) идентификация
b) аудит
c) аутентификация
d) авторизация

36. Проверка подлинности пользователя по предъявленному им идентификатору — это
a) авторизация
b) аутентификация
c) аудит
d) идентификация

37. Свойство, которое гарантирует, что информация не может быть доступна или раскрыта для неавторизованных личностей, объектов или процессов — это
a) детерминированность
b) достоверность
c) целостность
d) конфиденциальность

38. Система, позволяющая разделить сеть на две или более частей и реализовать набор правил, определяющих условия прохождения пакетов из одной части в другую, называется
a) брандмауэром
b) браузером
c) маршрутизатором
d) фильтром

39. Компьютерным вирусом называется:

a) любая программа, созданная на языках низкого уровня

b) небольшая программа, способная к самокопированию, которая может приписывать себя к другим программам

c) файл, содержащий макросы

d) нет правильного ответа

40. Что из нижеперечисленного является одним из способов защиты информации на компьютере?

a) защита паролем данных

b) дефрагментация жесткого диска

c) полное отключение системного блока

d) переустановка операционной системы

e) нет правильного ответа

f) все ответы правильные

41. Что такое руткит?

a) вредоносная программа, отслеживающая, какие сайты посещает пользователь

b) программа, блокирующая доступ к компьютеру и требующая деньги за разблокировку

c) программа для скрытого взятия под контроль взломанной системы

d) нет правильного ответа

e) все ответы верны

42. Под фишингом понимают

a) рассылки от имени популярных компаний или организаций, содержащих ссылки на ложные сайты, внешне неотличимые от настоящих.

b) перераспределение файлов и логической структуры диска

c) преобразование информации в целях скрытия от неавторизованных лиц

d) нет правильного ответа

e) все ответы верны

43. Как называется информация, круг лиц, имеющих доступ к которой ограничен?

a) открытая

b) конфиденциальная

c) зашифрованная

44. Шифрование информации это - ...

a) преобразование информации, при котором содержание становится непонятным для не обладающих соответствующими полномочиями субъектов

b) преобразование информации в двоичный код

c) процесс сжатия информации, с целью уменьшения занимаемого ей объема на диске

d) все ответы верны

e) нет правильного ответа

45. Что называют защитой информации?

a) предотвращение утечки информации

b) предотвращение несанкционированных действий

c) предотвращение непреднамеренных воздействий на защищаемую информацию

d) все ответы верны

46. Что понимают под утечкой информации?

a) бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

b) преднамеренная порча или уничтожение информации

c) преднамеренное овладение конфиденциальной информацией лицом, не имеющим права доступа к данным.

6 семестр

1. Какая из приведенных техник является самой важной при выборе конкретных защитных мер?

a) Анализ рисков
b) Анализ затрат / выгоды
c) Результаты ALE
d) Выявление уязвимостей и угроз, являющихся причиной риска

2. Что лучше всего описывает цель расчета ALE?

a) Количественно оценить уровень безопасности среды
b) Оценить возможные потери для каждой контрмеры
c) Количественно оценить затраты / выгоды
d) Оценить потенциальные потери от угрозы в год

3. Тактическое планирование – это:

a) Среднесрочное планирование
b) Долгосрочное планирование
c) Ежедневное планирование
d) Планирование на 6 месяцев

4. Что является определением воздействия (exposure) на безопасность?

a) Нечто, приводящее к ущербу от угрозы
b) Любая потенциальная опасность для информации или систем
c) Любой недостаток или отсутствие информационной безопасности
d) Потенциальные потери от угрозы

5. Как рассчитать остаточный риск?

a) Угрозы x Риски x Ценность актива
b) (Угрозы x Ценность актива x Уязвимости) x Риски
c) SLE x Частоту = ALE
d) (Угрозы x Уязвимости x Ценность актива) x Недостаток контроля

6. Что из перечисленного не является целью проведения анализа рисков?

a) Делегирование полномочий
b) Количественная оценка воздействия потенциальных угроз
c) Выявление рисков
d) Определение баланса между воздействием риска и стоимостью необходимых контрмер

7. Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?

a) Поддержка
b) Выполнение анализа рисков
c) Определение цели и границ
d) Делегирование полномочий

8. Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?

a) Чтобы убедиться, что проводится справедливая оценка
b) Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ
c) Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа
d) Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку

9. Что является наилучшим описанием количественного анализа рисков?

a) Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности
b) Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков
c) Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков
d) Метод, основанный на суждениях и интуиции

10. Почему количественный анализ рисков в чистом виде не достижим?

a) Он достижим и используется
b) Он присваивает уровни критичности. Их сложно перевести в денежный вид.
c) Это связано с точностью количественных элементов
d) Количественные измерения должны применяться к качественным элементам

11. Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?

a) Много информации нужно собрать и ввести в программу
b) Руководство должно одобрить создание группы
c) Анализ рисков не может быть автоматизирован, что связано с самой природой оценки
d) Множество людей должно одобрить данные

12. Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?

a) Стандарты
b) Должный процесс (Due process)
c) Должная забота (Due care)
d) Снижение обязательств

13. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?

a) Список стандартов, процедур и политик для разработки программы безопасности
b) Текущая версия ISO 17799
c) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
d) Открытый стандарт, определяющий цели контроля

14. Из каких четырех доменов состоит CobiT?
a) Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
b) Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка
c) Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка
d) Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка

15. Что представляет собой стандарт ISO/IEC 27799?
a) Стандарт по защите персональных данных о здоровье
b) Новая версия BS 17799
c) Определения для новой серии ISO 27000
d) Новая версия NIST 800-60

16. CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?
a) COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам
b) COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень
c) COSO учитывает корпоративную культуру и разработку политик
d) COSO – это система отказоустойчивости

17. OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами?
a) NIST и OCTAVE являются корпоративными
b) NIST и OCTAVE ориентирован на ИТ
c) AS/NZS ориентирован на ИТ
d) NIST и AS/NZS являются корпоративными

18. Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?
a) Анализ связующего дерева
b) AS/NZS
c) NIST
d) Анализ сбоев и дефектов

20. Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?
a) Безопасная OECD
b) ISO\IEC
c) OECD

d) CPTED

21. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:
a) гаммирования;
b) подстановки;
c) кодирования;
d) перестановки;
e) аналитических преобразований.

22. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:
a) гаммирования;
b) подстановки;
c) кодирования;
d) перестановки;
e) аналитических преобразований.

23. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:
a) гаммирования;
b) подстановки;
c) кодирования;
d) перестановки;
e) аналитических преобразований.

24. Пространство ключей k – это…
a) набор возможных значений ключа
b) длина ключа
c) нет правильного ответа

25. Криптосистемы разделяются на:
a) симметричные
b) ассиметричные
c) с открытым ключом
d) не полностью симметричные

26. Сколько используется ключей в симметричных криптосистемах для шифрования и дешифрования
a) 1
b) 2
c) 3

27. Сколько ключей используется в системах с открытым ключом
a) 2
b) 3
c) 1

28. Как связаны ключи друг с другом в системе с открытым ключом
a) математически
b) логически
c) алгоритмически

29. Электронной подписью называется…
   a) присоединяемое к тексту его криптографическое преобразование
   b) текст
   c) зашифрованный текст

30. Криптостойкость – это…
   a) характеристика шрифта, определяющая его стойкость к дешифрованию без знания ключа
   b) свойство гаммы
   c) все ответы верны

31. Показатели криптостойкости:
   a) количество всех возможных ключей
   b) среднее время, необходимое для криптоанализа
   c) количество символов в ключе

32. Для современных криптографических систем защиты информации сформулированы следующие общепринятые требования:
   a) знание алгоритма шифрования не должно влиять на надежность защиты
   b) структурные элементы алгоритма шифрования должны быть неизменными
   c) не должно быть простых и легко устанавливаемых зависимостью между ключами последовательно используемыми в процессе шифрования
   d) длина шифрованного текста должна быть равной лине исходного текста
   e) зашифрованное сообщение должно поддаваться чтению только при наличии ключа
   f) нет правильного ответа

33. Основные современные методы шифрования:
   a) алгоритма гаммирования
   b) алгоритмы сложных математических преобразований
   c) алгоритм перестановки

34. Символы исходного текста складываются с символами некой случайной последовательности – это…
   a) алгоритм гаммирования
   b) алгоритм перестановки
   c) алгоритм аналитических преобразований

35. Символы оригинального текста меняются местами по определенному принципу, являющемуся секретным ключом – это…
   a) алгоритм перестановки
   b) алгоритм подстановки
   c) алгоритм гаммрования

36. Самой простой разновидность подстановки является
   a) простая замена
   b) перестановка
   c) простая перестановка

37. Из скольки последовательностей состоит расшифровка текста по таблице Вижинера

a) 3
b) 4
c) 5

38. Какие таблицы Вижинера можно использовать для повышения стойкости шифрования
a) во всех (кроме первой) строках таблицы буквы располагаются в произвольном порядке
b) в качестве ключа используется случайность последовательных чисел
c) нет правильного ответа

39. В чем суть метода перестановки
a) символы шифруемого текста переставляются по определенным правилам внутри шифруемого блока символов
b) замена алфавита
c) все правильные

40. Сколько существует способов гаммирования
a) 2
b) 5
c) 3

41. Чем определяется стойкость шифрования методом гаммирования
a) свойством гаммы
b) длина ключа
c) нет правильного ответа

42. Что может использоваться в качестве гаммы
a) любая последовательность случайных символов
b) число
c) все ответы верны

43. Какой метод используется при шифровании с помощью аналитических преобразований
a) алгебры матриц
b) матрица
c) факториал

44. Что используется в качестве ключа при шифровании с помощью аналитических преобразований
a) матрица A
b) вектор
c) обратная матрица

45. Как осуществляется дешифрование текста при аналитических преобразованиях
a) умножение матрицы на вектор
b) деление матрицы на вектор
c) перемножение матриц

46. Комбинации комбинированного метода шифрования:
a) подстановка+гаммирование
b) гаммирование+гаммирование

c) подстановка+перестановка

47. Для чего использовался DES-алгоритм из-за небольшого размер ключа
    a) закрытия коммерческой информации
    b) шифрования секретной информации
    c) нет правильного ответа

48. Основные области применения DES-алгоритма
    a) хранение данных на компьютере
    b) электронная система платежей
    c) аутентификация сообщений

49. Достоинства ГОСТа 28147-89
    a) высокая стойкость
    b) цена
    c) гибкость

50. Чем отличается блок-схема алгоритма ГОСТ от блок-схемы DES-алгоритма
    a) отсутствием начальной перестановки и числом циклов шифрования
    b) длиной ключа
    c) методом шифрования

51. Ключ алгоритма ГОСТ – это…
    a) массив, состоящий из 32-мерных векторов
    b) последовательность чисел
    c) алфавит

52. Какой ключ используется в шифре ГОСТ
    a) 256-битовый
    b) 246-битовый
    c) 356-битовый

53. Примеры программных шифраторов:
    a) PGP
    b) BestCrypt 6.04
    c) PTR

54. Плюсы программных шифраторов:
    a) цена
    b) гибкость
    c) быстродействие

55. УКЗД – это…
    a) устройство криптографической защиты данных
    b) устройство криптографической заданности данных
    c) нет правильного ответа

56. Блок управления – это…
    a) основной модуль шифратора, который «заведует» работой всех остальных
    b) устройство криптографической заданности данных
    c) проходной шифратор

57. Вычислитель – это…

a) набор регистров, сумматоров, блоков подстановки, связанных собой шинами передачи данных
b) файлы, использующие различные методы кэширования
c) язык описания данных

58. Блок управления – это…
a) аппаратно реализованная программа, управляющая вычислителем
b) язык описания данных
c) процесс определения отвечает на текущее состояние разработки требованиям данного этапа

59. Какой шифратор можно использовать для защиты передаваемой в Сеть информации
a) обычный шифратор
b) проходной шифратор
c) табличный шифратор

60. Из каких структурных единиц состоит шифропроцессор
a) вычислитель
b) блок управления
c) буфер ввода-вывода

61. Криптографические действия выполняет…
a) вычислитель
b) буфер ввода-вывода
c) блок управления

62. Наиболее известные разновидности полиалфавита:
a) одноконтурные
b) многоконтурные
c) поликонтурные

63. Устройство, дающее статически случайный шум – это…
a) генератор случайных чисел
b) контроль ввода на компьютер
c) УКЗД

64. Какие дополнительные порты ввода-вывода содержит УКЗД:
a) COM
b) USB
c) FGR

65. Сколько существует перестановок в стандарте DES
a) 3
b) 4
c) 2

66. Какие перестановки существуют в стандарте DES
a) простые
b) расширенные

c) сокращенные

Задания в форме практических работ. Комплект разноуровневых задач (заданий)

Задание № 1

1 Информационная безопасность. Основные определения.

2 Особенности парольных систем аутентификации: рекомендации по практической реализации парольных систем, оценка стойкости парольных систем, методы хранения паролей.

3 Протоколирование и аудит.

4 Формальные модели целостности: .модель Кларка-Вилсона, модель Биба.

5 Структура государственных органов, обеспечивающих политику информационной безопасности в России.

Задание № 2

1 Угрозы информационной безопасности.

2 Методы разграничения доступа.

3 Построение систем защиты от угроз нарушения целостности: типовая структура такой системы.

4 Ролевая модель управления доступом

5 Структура государственных органов, обеспечивающих политику информационной безопасности в России

Вопросы к зачету

1. Основные понятия защиты информации и информационной безопасности
2. Анализ угроз информационной безопасности
3. Проблемы безопасности IP-сетей
4. Угрозы и уязвимости проводных корпоративных сетей
5. Угрозы и уязвимости беспроводных сетей
6. Способы обеспечения информационной безопасности
7. Основные понятия политики безопасности
8. Структура политики безопасности организации. Базовая политика безопасности. Специализированные политики безопасности. Процедуры безопасности
9. Роль стандартов информационной безопасности
10. Стандарты ISO/IEC 17799:2002 (BS 7799:2000)
11. Стандарт BSI
12. Международный стандарт ISO 15408 «Общие критерии безопасности информационных технологий»
13. Стандарты для беспроводных сетей
14. Стандарты информационной безопасности в Интернете
15. Отечественные стандарты безопасности информационных технологий
16. Основные понятия криптографической защиты информации
17. Симметричные криптосистемы шифрования
18. Асимметричные криптосистемы шифрования
19. Комбинированная криптосистема шифрования
20. Электронная цифровая подпись и функция хэширования

21. Управление криптоключами
22. Классификация криптографических алгоритмов
23. Симметричные алгоритмы шифрования. Блочные алгоритмы шифрования данных
24. Асимметричные криптоалгоритмы. Алгоритм шифрования RSA. Алгоритмы цифровой подписи
25. Аутентификация, авторизация и администрирование действий пользователей
26. Методы аутентификации, использующие пароли и PIN-коды
27. Строгая аутентификация
28. Биометрическая аутентификация пользователя
29. Угрозы безопасности ОС
30. Понятие защищенной ОС
31. Основные функции подсистемы защиты ОС
32. Идентификация, аутентификация и авторизация субъектов доступа
33. Разграничение доступа к объектам ОС
34. Аудит безопасности в ОС.

Вопросы к экзамену

1. Основные понятия защиты информации и информационной безопасности
2. Анализ угроз информационной безопасности
3. Анализ угроз сетевой безопасности.
4. Способы обеспечения информационной безопасности
5. Основные понятия политики безопасности.
6. Структура политики безопасности организации. Процедуры безопасности
7. Разработка политики безопасности.
8. Стандарты информационной безопасности
9. Основные понятия криптографической защиты информации
10. Симметричные криптосистемы шифрования
11. Асимметричные криптосистемы шифрования
12. Комбинированная криптосистема шифрования
13. Электронная цифровая подпись и функция хэширования
14. Управление криптоключами
15. Аутентификация, авторизация и администрирование действий пользователей
16. Безопасность КИС.
17. Безопасность облачных вычислений.
18. Обеспечение безопасности ОС.
19. Функции межсетевых экранов
20. Особенности функционирования
21. Схемы сетевой защиты на базе МЭ
22. Концепция построения виртуальных защищенных сетей VPN
23. VPN-решения для построения защищенных сетей
24. Протоколы формирования защищенных каналов на канальном уровне
25. Протоколы формирования защищенных каналов на сеансовом уровне
26. Защита беспроводных сетей
27. Архитектура средств безопасности IPSec. Защита передаваемых данных с помощью протоколов AH и ESP
28. Протокол управления криптоключами IKE

29. Основные схемы применения IPSec. Преимущества средств безопасности IPSec
30. Управление идентификацией и доступом
31. Организация защищенного удаленного доступа. Централизованный контроль удаленного доступа
32. Управление доступом по схеме однократного входа с авторизацией Single Sign-On (SSO)
33. Протокол Kerberos
34. Инфраструктура управления открытыми ключами PKI
35. Технология анализа защищенности
36. Технологии обнаружения атак
37. Компьютерные вирусы и проблемы антивирусной защиты.
38. Концепция адаптивного управления безопасностью.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения	Измененные пункты	Решение Учебно-методического совета