МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Директор НТИ (филиал) СКФУ
_____ Ефанов А.В
«__»_____ 2022 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине

«Информационная безопасность и передача данных»

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Направление подготовки	15.04.04 Автоматизация технологических процессов и производств
Направленность (профиль)	Информационно-управляющие системы
Форма обучения	очно-заочная
Год начала обучения	2022
Изучается в 5 семестре	

Предисловие

1. Назначение: фонд оценочных средств по дисциплине «Защита информации в системах управления» предназначен для оценки знаний обучающихся при освоении ими дисциплины при проведении текущего контроля успеваемости и промежуточной аттестации. Фонд включает в себя вопросы для собеседования при проведении практических и лабораторных занятий и вопросы к экзамену.

2. Фонд оценочных средств текущего контроля успеваемость и промежуточной аттестации на основе рабочей программы дисциплины «Защита информации в системах управления» в соответствии с образовательной программой по направлению подготовки 15.04.04 Автоматизация технологических процессов и производств, утвержденной на заседании Учёного совета СКФУ протокол №____ от «__»_____ 2022 г.

3. Разработчик: Кочеров Ю.Н. , доцент ИСЭиА

4. ФОС рассмотрен и утвержден на заседании кафедры информационных систем, электропривода и автоматики, протокол №____ от «__»_____ 2022 г.

5. Проведена экспертиза ФОС. Члены экспертной группы, проводившие внутреннюю экспертизу:

Председатель
Д.И. Лищенко, ведущий специалист ЦЦРТО КИПиА АО «Невинномысский Азот»
Члены экспертной группы
А.И. Колдаев, зав. кафедрой ИСЭА
Д.В. Болдырев, доцент кафедры ИСЭА

Экспертное заключение: фонд оценочных средств может быть использован для проведения текущего контроля успеваемости и промежуточной аттестации обучающихся по направлению подготовки 15.04.04 Автоматизация технологических процессов и производств.

«____»_____ 2022 г. _ _____
(подпись)

6. Срок действия ФОС: 1 год

Паспорт фонда оценочных средств
для проведения текущего контроля успеваемости и промежуточной аттестации

По дисциплине Защита информации в системах управления систем
Направление подготовки 15.04.04 Автоматизация технологических процессов и производств
Направленность (профиль) Информационно-управляющие системы
Квалификация выпускника магистр
Форма обучения очно-заочная
Учебный план 2022г.

Код оцениваемой компетенции (или её части)	Модуль, раздел, тема (в соответствии с Программой)	Тип контроля	Вид контроля	Компонент фонда оценочных средств	Количество заданий для каждого уровня, шт.	
					Базовый	Продвинутый
ПК-9	Информационная безопасность информационных систем	текущий	Устный опрос	Вопросы для собеседования	40	37
ПК-9	Средства реализации защиты в информационных системах	текущий	Устный опрос	Вопросы для собеседования	16	14

Составитель _____ Ю.Н. Кочеров
(подпись)

«____»_____ 2022 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
Директор НТИ (филиал) СКФУ
_____ Ефанов А.В
«__»_____ 2022 г.

Вопросы для собеседования

по дисциплине «Защита информации в системах управления»
Базовый уровень

1. Обеспечение информационной безопасности.
2. Угрозы информационной безопасности.
3. Услуги безопасности.
4. Механизмы реализации услуг безопасности.
5. Администрирование.
6. Протоколирование и аудит.
7. Структура правовой защиты информации.
8. Оценка надежности систем защиты информации. Интенсивность отказов. Время восстановления.
9. Задачи и методы резервирования.
10. Добавочная защита информации.
11. Критерий и параметры проектирования оптимальной системы защиты.
12. Защищенность системы с точки зрения риска.
13. Основной критерий защищенности.
14. Этапы проектирования системы защиты.
15. Этапы оценки защищенности и выбора оптимального варианта системы защиты.
16. Подходы к проектированию систем защиты, обладающих избыточных механизмом.
17. Системный подход к проектированию систем защиты.
18. Архитектуры сетевой системы защиты. Распределенная, централизованная, централизованно-распределенная архитектуры.
19. Периодическое обновление секрета.
20. Криптографические алгоритмы, схемы и системы.
21. Пространственное и временное разделение секрета.
22. Пороговые схемы разделения секрета.
23. Симметричные и асимметричные криптографические системы.
24. Криптографическая система RSA. Эффективность реализации.
25. Криптосистема RSA. Атаки на RSA.
26. Что такое LFSR?
27. Как построить псевдослучайный генератор на основе регистра сдвига?
28. На чем базируется стойкость генераторов псевдослучайных чисел, исследованных в лабораторной работе?
29. Что такое симметричное шифрование?
30. В чем особенность блочных шифров?
31. Какова длина ключа блочного шифра?
32. В чем особенность асимметричных систем шифрования?
33. На чем базируется криптостойкость RSA?

34. Назначение цифровой подписи.
35. В чем отличие криптосхемы ЭльГамаля от RSA?
36. Перечислить виды атак на пароли.
37. Перечислить критерии стойкости парольной защиты.
38. Перечислить и охарактеризовать методы противостояния атаке полным перебором.
39. Охарактеризовать влияние длины пароля на вероятность раскрытия.
40. Назначение протокола IPSec.
41. Состав семейства протоколов IPSec.
42. Средства настройки IPSec в Windows 2000/XP.
43. Состав политики безопасности.
44. Опишите утилиту ping, методы и случаи ее применения.
45. Описать данные, полученные о компьютере с помощью XSpider
46. Опишите типы уязвимостей компьютерных систем
47. Как можно предотвратить появление таких уязвимостей с помощью изученных средств?
48. Описать известные типы МСЭ и отличия между ними.
49. Этапы и средства реализации атак. Классификация атак.
50. Таксономия систем обнаружения атак.
51. Сформулировать алгоритм сигнатурного поиска вредоносного ПО.
52. Сформулировать алгоритм эвристического поиска вредоносного ПО.
53. Сформулировать алгоритм работы веб-сканера антивируса
54. Сформулировать алгоритм работы почтового сканера антивируса.
55. Каким способом возможен запуск серверной части СУБД.
56. Что такое привилегия. Каково её предназначение.

Продвинутый уровень

1. Разбалансированная RSA. Пакетная RSA. Ограничения при использовании RSA.
2. Криптосистема ЭльГамаля.
3. Методы экспоненциального ключевого обмена Диффи-Хеллмана.
4. Защита информации и сетевых ресурсов в сетях, подключенных к Internet. Классификация атак, направленных против узла или сети.
5. Прослушивание, сканирование сети и генерация пакетов.
6. Перехват данных на базе ложных ARP ответов, навязывания ложного маршрутизатора (ложное сообщение ICMP Redirect, атака при конфигурировании хоста, атака на протоколы маршрутизатора).
7. Имперсонация без обратной связи, на базе десинхронизации TCP-соединения.
8. Несанкционированное подключение к сети.
9. Несанкционированный обмен данными: туннелирование, атака крошечными фрагментами.
10. Отказ в обслуживании.
11. Межсетевые экраны. Классификация. Применение МЭ. Виды подключения МЭ.
12. Защита информации в автоматизированных системах на предприятии. Основные принципы построения системы защиты информации в ИС.
13. Программные средства защиты информации. Классификация.
14. Методы опознавания ИС и ее элементов пользователем. Проблемы регулирования использования ресурсов.
15. Программы защиты программ. Защита от копирования. Программы ядра системы безопасности.
16. Классификация угроз перевода СЗ в пассивное состояние.
17. Методы противодействия загрузке ОС без ПО СЗ.

18. Реализация программно-аппаратного мониторинга активности СЗ.
19. Механизм удаленного (сетевого) мониторинга активности.
20. Защита электронной почты.
21. Защита электронных платежей.
22. Программа информационной безопасности России и пути ее реализации.
23. Формирование государственной политики в области обеспечения информационной безопасности Российской Федерации.
24. Подготовка предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации.
25. Разработка целевых программ обеспечения информационной безопасности Российской Федерации.
26. Какие тесты на случайность вам известны?
27. Как реализовать возведение в степень чисел большой разрядности по большому модулю?
28. Сравните результаты тестов генераторов из первой лабораторной работы с тестами второй работы.
29. На чем базируется криптостойкость блочного шифра?
30. Какие элементарные операции используются в симметричном шифровании?
31. Как увеличить производительность системы шифрования RSA?
32. Какие атаки на систему RSA вам известны?
33. Как противодействовать атакам на систему RSA?
34. На чем базируется криптостойкость системы ЭльГамаля?
35. Сформировать рекомендации по составлению паролей.
36. Перечислить типы угроз безопасности парольных систем.
37. Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет.
38. Определить время перебора всех паролей, состоящих из 6 цифр
39. Создание правил и фильтров для политики безопасности.
40. Возможные методы проверки подлинности IPSec.
41. Возможные места хранения назначенных политик безопасности.
42. Совместное применение систем обнаружения атак и других средств защиты.
43. Методы обнаружения аномалий: статистический анализ, нейросетевые методы, анализ изменения критических параметров во времени.
44. Анализ журналов регистрации и сетевого трафика.
45. Анализ заголовков, процессов, сервисов и портов.
46. Настроить NetFlow на маршрутизаторе.
47. Разработать и осуществить эмпирический анализ алгоритма сортировки простыми вставками.
48. Разработать и осуществить эмпирический анализ алгоритма бинарной сортировки.
49. Разработать алгоритм быстрой сортировки двумерного массива и осуществить математический анализ.
50. Разработать алгоритм пирамидальной сортировки двумерного массива и осуществить математический анализ.
51. Какие основные утилиты входят в состав СУБД, какие функции они выполняют.

Критерии оценки:

Оценка «зачтено» выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения. Допускаются некоторые неточности, недостаточно правильные формулировки в изложении программного материала, затруднения при выполнении практических работ.
Оценка «не зачтено» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы.

Составитель _____ Ю.Н. Кочеров
(подпись)

«____»_____ 2022 г.