Подписан: Ефанов Алексей Валерьевич
Дата: 2022-06-27 16:38:31

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

УТВЕРЖДАЮ
Директор НТИ (филиала) СКФУ
_____А.В. Ефанов
"___"_____2022 г

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине
Информационная безопасность автоматизированных систем

Направление подготовки	15.03.04 Автоматизация технологических процессов и производств
Направленность (профиль)	Информационно-управляющие системы
Форма обучения	очная
Год начала обучения	2022
Реализуется в 7 семестре	

Введение

1. Назначение: обеспечение методической основы для организации и проведения текущего контроля по дисциплине «Информационная безопасность автоматизированных систем». Текущий контроль по данной дисциплине – вид систематической проверки знаний, умений, навыков студентов. Задачами текущего контроля являются получение первичной информацию о ходе и качестве освоения компетенций, а также стимулирование регулярной целенаправленной работы студентов. Для формирования определенного уровня компетенций.

2. ФОС является приложением к программе дисциплины «Информационная безопасность автоматизированных систем» и в соответствии с образовательной программой высшего образования по направлению подготовки 15.03.04 Автоматизация технологических процессов и производств.

3. Разработчик: Кочеров Юрий Николаевич, доцент базовой кафедры Регионального индустриального парка, кандидат технических наук

4. Проведена экспертиза ФОС.

Члены экспертной группы:

Председатель:
Мельникова Е.Н. – председатель УМК НТИ (филиал) СКФУ

Члены комиссии:
А.И. Колдаев, и.о. зав. кафедрой информационных систем, электропривода и автоматики
Д.В. Болдырев, доцент кафедры информационных систем, электропривода и автоматики

Представитель организации-работодателя:
Остапенко Н.А., к.т.н., ведущий конструктор КИЭП «Энергомера» филиал АО «Электротехнические заводы «Энергомера»

Экспертное заключение: фонд оценочных средств соответствует ОП ВО по направлению подготовки 15.03.04 Автоматизация технологических процессов и производств и рекомендуется для оценивания уровня сформированности компетенций при проведении текущего контроля успеваемости и промежуточной аттестации студентов по дисциплине «Информационная безопасность автоматизированных систем».

05 марта 2022 г.

5. Срок действия ФОС определяется сроком реализации образовательной программы.

1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

Код оцениваемой компетенции, индикатора (ов)	Этап формирования компетенции (№ темы) *(в соответствии с рабочей программой дисциплины)*	Средства и технологии оценки	Вид контроля, аттестация *(текущий/промежуточный)*	Тип контроля *(устный, письменный или с использованием технических средств)*	Наименование оценочного средства
ИД-1 ПК-3	1-9	Собеседование	Текущий	Устный	Вопросы для собеседования
ИД-1 ПК-3	1-9	Экзамен	Промежуточный	Устный	Вопросы для экзамена

2. Описание показателей и критериев оценивания на различных этапах их формирования, описание шкал оценивания

Уровни сформированности компетенци(ий), индикатора (ов)	Дескрипторы			
	Минимальный уровень не достигнут (Неудовлетворительно) 2 балла	Минимальный уровень (удовлетворительно) 3 балла	Средний уровень (хорошо) 4 балла	Высокий уровень (отлично) 5 баллов
ПК-3. Способен использовать средства и системы автоматизации, контроля, диагностики, испытаний, управления производством, жизненным циклом продукции и ее качеством.				
Результаты обучения по дисциплине (модулю): *Индикатор:* ИД-1 ПК-3	На недостаточном уровне использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности, включая системное,	На низком уровне использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности,	Использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности,	Использует на высоком уровне современные подходы, принципы и методы создания информационных систем защиты данных, технического

	функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации	включая системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации	включая системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации	и программного обеспечения систем безопасности, включая системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации

Описание шкалы оценивания

В рамках рейтинговой системы успеваемость студентов по каждой дисциплине оценивается в ходе текущего контроля и промежуточной аттестации.

Текущий контроль

Рейтинговая оценка знаний студента (в случаях, предусмотренных нормативными актами СКФУ).

№ п/п	Вид деятельности студентов	Сроки выполнения	Количество баллов
7 семестр			
1	Собеседование по темам 1-4, Защита лабораторных работ	8	25
2	Собеседование по теме 5-8, Защита лабораторных работ	16	30
	Итого за __ семестр:		55
	Итого:		55

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	***Рейтинговый балл (в % от максимального балла за контрольное задание)***
Отличный	***100***
Хороший	***80***
Удовлетворительный	***60***

Неудвлетворительный	***0***

Промежуточная аттестация

Промежуточная аттестация в форме **экзамена** предусматривает проведение обязательной экзаменационной процедуры и оценивается 40 баллами из 100. Положительный ответ студента на экзамене оценивается рейтинговыми баллами в диапазоне от **20** до **40** (**20** ≤ $S_{экз}$ ≤ **40**), оценка **меньше 20** баллов считается неудовлетворительной.

Шкала соответствия рейтингового балла экзамена 5-балльной системе

Рейтинговый балл по дисциплине	**Оценка по 5-балльной системе**
35 – 40	Отлично
28 – 34	Хорошо
20 – 27	Удовлетворительно

Итоговая оценка по дисциплине, изучаемой в одном семестре, определяется по сумме баллов, набранных за работу в течение семестра, и баллов, полученных при сдаче экзамена:

Шкала пересчета рейтингового балла по дисциплине в оценку по 5-балльной системе

Рейтинговый балл по дисциплине	***Оценка по 5-балльной системе***
88 – 100	*Отлично*
72 – 87	*Хорошо*
53 – 71	*Удовлетворительно*
< ***53***	*Неудовлетворительно*

Промежуточная аттестация в форме **курсовой работы (проекта)**

Максимальная сумма баллов по **курсовой работе (проекту)** устанавливается в **100** баллов и переводится в оценку по 5-балльной системе в соответствии со шкалой:

Шкала соответствия рейтингового балла 5-балльной системе

Рейтинговый балл	**Оценка по 5-балльной системе**
88 – 100	Отлично
72 – 87	Хорошо
53 – 71	Удовлетворительно
< 53	Неудовлетворительно

3. Типовые контрольные задания и иные материалы, характеризующие этапы формирования компетенций

Вопросы для собеседования

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.
57. Разбалансированная RSA. Пакетная RSA. Ограничения при использовании RSA.
58. Криптосистема ЭльГамаля.
59. Методы экспоненциального ключевого обмена Диффи-Хеллмана.

60. Защита информации и сетевых ресурсов в сетях, подключенных к Internet. Классификация атак, направленных против узла или сети.
61. Прослушивание, сканирование сети и генерация пакетов.
62. Перехват данных на базе ложных ARP ответов, навязывания ложного маршрутизатора (ложное сообщение ICMP Redirect, атака при конфигурировании хоста, атака на протоколы маршрутизатора).
63. Имперсонация без обратной связи, на базе десинхронизации TCP-соединения.
64. Несанкционированное подключение к сети.
65. Несанкционированный обмен данными: туннелирование, атака крошечными фрагментами.
66. Отказ в обслуживании.
67. Межсетевые экраны. Классификация. Применение МЭ. Виды подключения МЭ.
68. Защита информации в автоматизированных системах на предприятии. Основные принципы построения системы защиты информации в ИС.
69. Программные средства защиты информации. Классификация.
70. Методы опознавания ИС и ее элементов пользователем. Проблемы регулирования использования ресурсов.
71. Программы защиты программ. Защита от копирования. Программы ядра системы безопасности.
72. Классификация угроз перевода СЗ в пассивное состояние.
73. Методы противодействия загрузке ОС без ПО СЗ.
74. Реализация программно-аппаратного мониторинга активности СЗ.
75. Механизм удаленного (сетевого) мониторинга активности.
76. Защита электронной почты.
77. Защита электронных платежей.
78. Программа информационной безопасности России и пути ее реализации.
79. Формирование государственной политики в области обеспечения информационной безопасности Российской Федерации.
80. Подготовка предложений по совершенствованию правового, методического, научно-технического и организационного обеспечения информационной безопасности Российской Федерации.
81. Разработка целевых программ обеспечения информационной безопасности Российской Федерации.
82. Какие тесты на случайность вам известны?
83. Как реализовать возведение в степень чисел большой разрядности по большому модулю?
84. Сравните результаты тестов генераторов из первой лабораторной работы с тестами второй работы.
85. На чем базируется криптостойкость блочного шифра?
86. Какие элементарные операции используются в симметричном шифровании?
87. Как увеличить производительность системы шифрования RSA?
88. Какие атаки на систему RSA вам известны?
89. Как противодействовать атакам на систему RSA?
90. На чем базируется криптостойкость системы ЭльГамаля?
91. Сформировать рекомендации по составлению паролей.
92. Перечислить типы угроз безопасности парольных систем.
93. Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время перебора которого было не меньше 10 лет.
94. Определить время перебора всех паролей, состоящих из 6 цифр
95. Создание правил и фильтров для политики безопасности.
96. Возможные методы проверки подлинности IPSec.
97. Возможные места хранения назначенных политик безопасности.

98. Совместное применение систем обнаружения атак и других средств защиты.
99. Методы обнаружения аномалий: статистический анализ, нейросетевые методы, анализ изменения критических параметров во времени.
100. Анализ журналов регистрации и сетевого трафика.
101. Анализ заголовков, процессов, сервисов и портов.
102. Настроить NetFlow на маршрутизаторе.
103. Разработать и осуществить эмпирический анализ алгоритма сортировки простыми вставками.
104. Разработать и осуществить эмпирический анализ алгоритма бинарной сортировки.
105. Разработать алгоритм быстрой сортировки двумерного массива и осуществить математический анализ.
106. Разработать алгоритм пирамидальной сортировки двумерного массива и осуществить математический анализ.
107. Какие основные утилиты входят в состав СУБД, какие функции они выполняют.

1. Критерии оценивания компетенций*

Оценка «отлично» выставляется студенту, если он
Использует на высоком уровне современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности, включая системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации.
Оценка «хорошо» выставляется студенту, если он
Использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности, включая системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации
Оценка «удовлетворительно» выставляется студенту, если он
На низком уровне использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности, включая системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации
Оценка «неудовлетворительно» выставляется студенту, если он
На недостаточном уровне использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности, включая системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации

2. Описание шкалы оценивания

Максимально возможный балл за весь текущий контроль устанавливается равным **55.** Текущее контрольное мероприятие считается сданным, если студент получил за него не менее 60% от установленного для этого контроля максимального балла. Рейтинговый балл, выставляемый студенту за текущее контрольное мероприятие, сданное студентом в установленные графиком контрольных мероприятий сроки, определяется следующим образом:

Уровень выполнения контрольного задания	Рейтинговый балл (в % от максимального балла за контрольное задание)
Отличный	**100**
Хороший	**80**
Удовлетворительный	**60**
Неудовлетворительный	**0**

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура проведения данного оценочного мероприятия включает в себя: защиту лабораторных работ

Предлагаемые студенту вопросы позволяют проверить компетенции ИД-1 ПК-3

Для подготовки к данному оценочному мероприятию необходимо 10 минут

При подготовке к ответу студенту предоставляется право отчетами о выпиленных лабораторных работах

При проверке задания, оцениваются последовательность и логика ответа и др.

Бланк оценочного листа собеседования

№ п/п	ФИО студента	Критерий оценивания			Итого
		правильность ответа	полнота раскрытия вопроса	умение аргументировать свой ответ	
1					
2					
…					

Вопросы к экзамену*

1. Защита информации в базах данных. Основные требования к информационной безопасности. Использование современных информационных технологий и методов для обеспечение информационной безопасности.
2. Введение в вопросы защиты информации. Информационная безопасность человека и общества.
3. Организационные меры защиты ЭВМ.
4. Анализ угроз сохранности информации.
5. Сопровождение комплексной системы защиты информации в автоматизированной системе (КСЗИ).
6. Разработка и реализация плана защиты информации. Суть задачи сопровождения
7. КСЗИ в АС. Служба защиты информации в АС как основной механизм организации сопровождения КСЗИ.
8. Организационные основы защиты информации в автоматизированных системах на предприятии.
9. Защита информационных и сетевых ресурсов в сетях, подключенных к Интернет.
10. Меры непосредственной защиты ЭВМ.
11. Защита аппаратных средств.
12. Криптографические методы защиты.
13. Значение криптографии в информационном обществе.
14. Симметричные системы шифрования.
15. Основы одно-ключевых криптосистем.
16. Принципы построения программных шифров.
17. Типы шифров.
18. Шифры с управляемыми операциями. Способ шифрования на основе управляемых перестановок.
19. Несимметричные системы шифрования.
20. Двухключевые шифры. Система открытого распределения ключей.
21. Защита операционной системы.
22. Процедуры проверки. Контроль доступа.
23. Защита информации в базах данных.

24. Нормативно-правовые документы, регламентирующие деятельность в области информационной безопасности. Государственная система защиты информации.
25. Проблемы организации работы вычислительного центра. Организационно-управленческие меры.
26. Экономические проблемы. Цели защиты ЭВМ и ответственность.
27. Характеристика методов и средств защиты информации. Порядок обеспечения защиты информации в автоматизированной системе (АС)
28. Правовые основы создания и деятельности службы защиты информации, ее основные задачи и функции.
29. Состав и содержание плана защиты, содержание мер и порядок его формирования и реализации.
30. Основные технические каналы утечки информации в автоматизированных системах. Меры и средства защиты элементов автоматизированных систем от утечки информации по техническим каналам.
31. Классификация уязвимостей; подходы определения уязвимостей безопасности сетей; сканеры для проверки уязвимостей фирм ISS, CISCO, NMAP и другие; защита сетей от компьютерных атак.
32. Распространенные атаки на системы связи (DoS, ping-of-death и т.д.). Методы и средства защиты; понятие адаптивного управления безопасностью сети.
33. Защита от стихийных бедствий. Защита от злоумышленников. Идентификация и
34. установление личности.
35. Защита памяти. Состояния выполнения программ. Применение микропроцессоров для защиты аппаратных средств.
36. Проблематика криптографии.
37. Одно-ключевые шифры.
38. Одно-ключевые модели шифрования.
39. Недетерминированные программные шифры.
40. Шифры с управляемыми подстановками.
41. Шифры на основе модифицирования подключей.
42. Цифровая электронная подпись. Хэш-функции на основе блочных шифров.
43. Вероятностные шифры. Гомофонические шифры.
44. Изоляция областей нарушения защиты операционной системы. Разработка и реализация операционных систем со средствами защиты.
45. Принятие решений о доступе. Организация доступа к базе данных. Назначение полномочий.

1. Критерии оценивания компетенций

Оценка «отлично» выставляется студенту, если он

Использует на высоком уровне современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности, включая системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации.

Оценка «хорошо» выставляется студенту, если он

Использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности, включая системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации

Оценка «удовлетворительно» выставляется студенту, если он

На низком уровне использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения

систем безопасности, включая системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации
Оценка «неудовлетворительно» выставляется студенту, если он
На недостаточном уровне использует современные подходы, принципы и методы создания информационных систем защиты данных, технического и программного обеспечения систем безопасности, включая системное, функциональное и прикладное программное обеспечение, а также аппаратные средства защиты информации

2. Описание шкалы оценивания

Промежуточная аттестация в форме экзамена предусматривает проведение обязательной экзаменационной процедуры и оценивается 40 баллами из 100. В случае если рейтинговый балл студента по дисциплине по итогам семестра равен 60, то программой автоматически добавляется 32 премиальных балла и выставляется оценка «отлично». Положительный ответ студента на экзамене оценивается рейтинговыми баллами в диапазоне от **20** до **40** (**20** $\leq S_{экз} \leq$ **40**), оценка **меньше 20** баллов считается неудовлетворительной.

Шкала соответствия рейтингового балла экзамена 5-балльной системе

Рейтинговый балл по дисциплине	**Оценка по 5-балльной системе**
35 – 40	Отлично
28 – 34	Хорошо
20 – 27	Удовлетворительно

3. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедура проведения экзамена осуществляется в соответствии с Положением о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся по образовательным программам высшего образования – программам бакалавриата, программам специалитета, программам магистратуры - в СКФУ.

В экзаменационный билет включаются 2 вопроса

Для подготовки по билету отводится 30 минут.