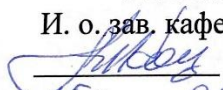


Документ подписан простой электронной подписью
Информация о владельце:
ФИО: Ефанов Алексей Валерьевич
Должность: Директор Невиномысского технологического института (филиал) СКФУ
Дата подписания: 12.10.2022 09:19:31
Уникальный программный идентификатор:
49214306dd433e7a1b0f8632f645f9d53c99e3d0

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

УТВЕРЖДАЮ
И. о. зав. кафедрой ИСЭиА
 Колдаев А.И.
«15» 03 2021 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

для проведения текущего контроля успеваемости и промежуточной аттестации по
дисциплине:

«Персональная кибербезопасность»

(ЭЛЕКТРОННЫЙ ДОКУМЕНТ)

Направление подготовки 09.03.02 Информационные системы и технологии
Профиль Информационные системы и технологии в бизнесе
Квалификация выпускника бакалавр
Форма обучения заочная
Год начала обучения 2021
Изучается на 1 курсе зимней сессии

Предисловие

1. Назначение: для проведения текущего контроля успеваемости и промежуточной аттестации по дисциплине «Персональная кибербезопасность» для студентов направления подготовки 09.03.02 Информационные системы и технологии.
2. Фонд оценочных средств текущего контроля успеваемости и промежуточной аттестации на основе рабочей программы дисциплины «Персональная кибербезопасность» в соответствии с образовательной программой по направлению подготовки 09.03.02 Информационные системы и технологии, утвержденной на заседании Учёного совета НТИ (филиал) СКФУ.
3. Разработчик: Кочеров Ю. Н. канд., техн., наук, доцент базовой кафедры регионального индустриального парка
4. ФОС рассмотрен и утвержден на заседании базовой кафедры регионального индустриального парка.
5. ФОС согласован с выпускающей кафедрой информационных систем, электропривода и автоматики.
6. Проведена экспертиза ФОС. Члены экспертной группы, проводившие внутреннюю экспертизу:

Председатель: Кузьменко В.В., и.о. директора НТИ (филиал) СКФУ, профессор кафедры гуманитарных и математических дисциплин

Члены экспертной группы:

Должикова М.В. – заместитель директора по учебно-воспитательной работе НТИ (филиал) СКФУ;

Колдаев А.И. – доцент кафедры информационных систем, электропривода и автоматики.

Эксперт, проводивший внешнюю экспертизу:

Остапенко Н.А., – кандидат технических наук, ведущий инженер-конструктор КБ модернизации ООО КИЭП «Энергомера» филиал АО «Электротехнические заводы «Энергомера»

7. Экспертное заключение: фонд оценочных средств отвечает основным требованиям федерального государственного образовательного стандарта и способствует формированию требуемых компетенций.

Срок действия ФОС: на срок реализации образовательной программы.

Паспорт фонда оценочных средств
для проведения текущего контроля успеваемости и промежуточной аттестации
дисциплине:
«Персональная кибербезопасность»

| | |
|--------------------------|---|
| Направление подготовки | 09.03.02 Информационные системы и технологии |
| Направленность (профиль) | Информационные системы и технологии в бизнесе |
| Квалификация выпускника | Бакалавр |
| Форма обучения | очная |
| Год начала обучения | 2021 г. |
| Изучается | на 1 курсе зимней сессии |

| Код оцениваемой компетенции | Этап формирования компетенции (№ темы) | Средства и технологии оценки | Вид контроля, аттестация | Тип контроля | Наименование оценочного средства |
|-----------------------------|--|------------------------------|--------------------------|--------------|----------------------------------|
| ПК-2 | Темы 1-6 | Собеседование | Текущий | Устный | Вопросы для собеседования |

Составитель Кочеров Ю.Н.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

**Вопросы для собеседования
по дисциплине Персональная кибербезопасность
Пороговый уровень**

Тема 1. История развития криптографии

- 1) Криптография древнего периода.
- 2) Криптография в средние века.

Тема 2. Основные понятия и определения информационной безопасности

- 1) В чем отличия Информации открытого и ограниченного доступа
- 2) Какая информация относится к конфиденциальной

Тема 3. Классификация угроз информационной безопасности

- 1) Источник угрозы – это...
- 2) Угроза (действие) – это...
- 3) Фактор (уязвимость) – это...
- 4) Последствия (атака) – это...

Тема 4. Методы защиты информации с применением симметричных алгоритмов шифрования

- 1) Методы защиты информации с применением симметричных алгоритмов шифрования
- 2) Виды алгоритмов симметричного шифрования
- 3) Достоинства и недостатки симметричного шифрования
- 4) Чем шифрование отличается от кодирования?
- 5) Должен ли быть секретным алгоритм шифрования?
- 6) Должен ли быть секретным ключ шифра при симметричном шифровании?
- 7) Кто может знать алгоритм шифрования?
- 8) Кто должен знать ключ шифра?
- 9) Опишите как получается матрица Виженера.
- 10) Опишите методику шифрования текста шифром Виженера.
- 11) Опишите методику шифрования с закрытым ключом.
- 12) Опишите логическую операцию XOR.

Тема 5. Методы защиты информации с применением асимметричных алгоритмов шифрования

- 1) Основные понятия и определения асимметричного шифрования
- 2) Принцип действия асимметричного шифрования
- 3) Применение асимметричных алгоритмов
- 4) В чем заключается алгоритм RSA?
- 5) Для чего и почему используют комбинированные криптоалгоритмы?

Тема 6. Методы защиты информации с применением методов основанных на разделении данных

- 1) Основные понятия и определения разделения данных
- 2) Методы разделения данных основанные на геометрических законах и численные примеры их реализации
- 3) Поясните концепцию разбиения данных. Приведите пример.
- 4) Поясните концепцию порогового разделения данных. Приведите пример.
- 5) Поясните преимущества использование системы остаточных классов для разделения секрета.
- 6) Каким образом информация из системы остаточных классов переводится в десятичную систему счисления с применением обобщенной полиадической системы счисления.

Повышенный уровень

Тема 1 История развития криптографии

- 1) Криптография в эпоху Возрождения (XIV-XVI вв.)
- 2) Криптография XVII-XX веков.
- 3) Современная криптография

Тема 2. Основные понятия и определения информационной безопасности

- 1) Что понимается под термином «Пользователь информации»
- 2) Что понимают под качеством информации

Тема 3. Классификация угроз информационной безопасности

- 1) Ущерб как категория классификации угроз
- 2) Классификация угроз информационной безопасност
- 3) Классификация источников угроз
- 4) Техногенные источники угроз
- 5) Ранжирование источников угроз

Тема 4. Методы защиты информации с применением симметричных алгоритмов шифрования

- 1) Область применения симметричного шифрования
- 2) Шифры перестановки. Анализ шифра простой перестановки.
- 3) Криптоанализ перестановок. Метод диграмм
- 4) Шифры замены. Анализ шифра замены.
- 5) Что делать, если размер ключа меньше размера текста?
- 6) В чем заключается идея шифра простой замены?
- 7) Алфавиты открытого текста и шифртекста совпадают или отличаются?
- 8) Как соотносятся частоты появления открытого текста и шифротекста?
- 9) Сколько уникальных вариантов ключа можно получить для заданного размера блока?
- 10) Опишите методику нахождения длинны ключевого слова.
- 11) Опишите методику нахождения ключевого слова если известна его длинна.
- 12) Механизм работы шифрования на основе XOR.
- 13) Насколько надежен рассмотренный алгоритм шифрования на основе XOR?

Тема 5. Методы защиты информации с применением асимметричных алгоритмов шифрования

- 1) Асимметричные алгоритмы
- 2) Надежность асимметричного шифрования
- 3) В чем заключаются достоинства и недостатки асимметричных алгоритмов?
- 4) В чем заключаются достоинства и недостатки симметричных алгоритмов?

Тема 6. Методы защиты информации с применением методов основанных на разделении данных

- 1) Основные понятия Системы остаточных классов
- 2) Методы разделения данных основанные на системе остаточных классов примеры их реализации
- 3) Расскажите принцип порогового разделения данных с применением схемы Шамира.
- 4) 4) Расскажите принцип порогового разделения данных с применением схемы Блэкли.
- 5) Расскажите принцип порогового разделения данных с применением схемы Миньотта.
- 6) Расскажите принцип порогового разделения данных с применением схемы Асмута-Блума.

Компетентностно-ориентированные задания

- 1) Используя таблицу частот, биграмм русского языка представленную в методических указаниях найдите какие пары букв встречаются чаще всего.
- 2) Используя ключевое слово «МАЙ» и таблицу Виженера представленную в методических указаниях расшифруйте следующий текст: «ЫРСОЕЫЛМСЬ».
- 3) Дано сообщение, представленное в десятичной системе счисления «1410» и ключ «1210» зашифруйте и расшифруйте его.
- 4) Для сообщения длиной 4 Вит выберите и обоснуйте простые числа для вычисления функции Эйлера и вычислите ее.
- 5) Для восстановления данных в схеме Блэкли необходимо решить систему уравнений
$$\begin{cases} 6x_1 + 5x_2 + 6x_3 = 340 \\ 9x_1 + 3x_2 + 1x_3 = 461 \\ 5x_1 + 1x_2 + 6x_3 = 282 \end{cases}$$
 Восстановите разделенные данные любым доступным Вам способом, представленные в системе.
- 6) Выберите и обоснуйте ряд чисел для представления числа «15» в системе остаточных классов

Составитель Кочеров Ю.Н.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

**Паспорт фонда тестовых заданий
по дисциплине Персональная кибербезопасность**

ПК-2 Способен выполнять работы по созданию (модификации) и сопровождению ИС, автоматизирующих задач организационного управления и бизнеспроцессов

| № п/п | Тест | Ключ |
|-------|---|---|
| 1. | Сведения в военной области относятся к: 1. коммерческой тайне; 2. персональным данным; 3. государственной тайне. | 3. государственной тайне |
| 2. | Персональные данные гражданина РФ относятся к... 1. государственной тайне; 2. коммерческой тайне; 3. общедоступной информации; 4. конфиденциальной информации. | 4. конфиденциальной информации |
| 3. | Как называется любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу? 1. личные данные; 2. индивидуальные данные; 3. субъективные данные; 4. персональные данные. | 4. персональные данные. |
| 4. | Информация о состоянии окружающей среды относится к... 1. государственной тайне; 2. коммерческой тайне; 3. конфиденциальной информации; 4. общедоступным сведениям. | 4. общедоступным сведениям. |
| 5. | Как называется информация или носитель информации, или информационный процесс, которые необходимо защищать в соответствии с поставленной целью защиты информации? 1. субъект защиты; 2. автоматизированная система; 3. объект информатизации; 4. объект защиты. | 4. объект защиты. |
| 6. | Какая логическая цепочка является корректной? 1. Источник угрозы - уязвимость - атака- угроза; 2. Источник угрозы - угроза - уязвимость - атака; 3. Угроза-уязвимость-источник угрозы-атака; 4. Источник угрозы - уязвимость-угроза-атака. | 4. Источник угрозы - уязвимость-угроза-атака. |
| 7. | Как называется слабость одного или нескольких активов, которая может быть использована одной или | 4. уязвимость. |

| | | |
|-----|--|----------------------------------|
| | <p>несколькими угрозами?</p> <ol style="list-style-type: none"> 1. источник угрозы; 2. атака; 3. ошибка; 4. уязвимость. | |
| 8. | <p>Как называется совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации?</p> <ol style="list-style-type: none"> 1. уязвимость; 2. источник угрозы; 3. атака; 4. угроза. | 4. угроза. |
| 9. | <p>Как называется попытка реализации угрозы?</p> <ol style="list-style-type: none"> 1. нападение; 2. уязвимость; 3. информационная война; 4. атака. | 4. атака. |
| 10. | <p>К какой категории по степени воздействия на объект защиты относятся угрозы, не нарушающие состав и нормальную работу объекта защиты?</p> <ol style="list-style-type: none"> 1. естественные; 2. искусственные; 3. активные; 4. пассивные. | 4. пассивные. |
| 11. | <p>К какой категории по степени воздействия на объект защиты относятся угрозы, нарушающие состав и нормальную работу объекта защиты?</p> <ol style="list-style-type: none"> 1. естественные; 2. искусственные; 3. пассивные; 4. активные. | 4. активные. |
| 12. | <p>Потенциальная возможность заражения информационной системы вирусом является примером...</p> <ol style="list-style-type: none"> 1. угрозы нарушения доступности; 2. угрозы нарушения конфиденциальности; 3. угрозы нарушения целостности. | 3. угрозы нарушения целостности. |
| 13. | <p>Потенциальная возможность повреждения оборудования из-за короткого замыкания является примером...</p> <ol style="list-style-type: none"> 1. угрозы нарушения целостности; 2. угрозы нарушения конфиденциальности; 3. угрозы нарушения доступности. | 3. угрозы нарушения доступности. |
| 14. | <p>Как называется доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники (СВТ) или автоматизированными системами (АС)?</p> <ol style="list-style-type: none"> 1. нелегальный доступ; 2. технический канал утечки; 3. неправомерный доступ; | 4. несанкционированный доступ; |

| | | |
|-----|---|---|
| | 4. несанкционированный доступ; | |
| 15. | Какой вид атаки направлен на получение конфиденциальной информации путем прослушивания сети? 1. сканирование сети; 2. навязывание ложного маршрута; 3. внедрение ложного объекта; 4. анализ сетевого трафика. | 4. анализ сетевого трафика. |
| 16. | Целью какой атаки является нарушение доступности информации для законных субъектов информационного обмена? 1. анализ сетевого трафика; 2. сканирование сети; 3. внедрение ложного объекта; 4. отказ в обслуживании. | 4. отказ в обслуживании. |
| 17. | Как называется воздействие на защищаемую информацию с помощью вредоносных программ? 1. программно-аналитическое воздействие; 2. программно-аппаратное воздействие; 3. технически-математическое воздействие; 4. программно-математическое воздействие. | 4. программно-математическое воздействие. |
| 18. | Как называется программа, которая, являясь частью другой программы с известными пользователю функциями, способна втайне от него выполнять некоторые дополнительные действия с целью причинения ему определенного ущерба? 1. вирус; 2. сетевой червь; 3. макровирус; 4. троянский конь. | 4. троянский конь. |
| 19. | Как называется вредоносная программа, распространяющаяся по сетевым каналам, способная к автономному преодолению систем защиты автоматизированных и компьютерных сетей, а также к созданию и дальнейшему распространению своих копий? 1. троянский конь; 2. вирус; 3. макровирус; 4. сетевой червь. | 4. сетевой червь; |
| 20. | По среде обитания вирусы подразделяются на: 1. файловые, загрузочные, аппаратные; 2. файловые, загрузочные; 3. файловые, сетевые, аппаратные; 4. файловые, загрузочные, сетевые. | 4. файловые, загрузочные, сетевые; |
| 21. | Вирус, написанный на макроязыке, встроенном в Word, называется... 1. полиморфным; 2. метаморфным; 3. файловым; 4. макровирусом. | 4. макровирусом. |
| 22. | В соответствии с ФЗ №149 "Об информации, | 4. общедоступная и |

| | | |
|-----|---|---|
| | <p>информационных технологиях и о защите информации" информация разделяется на следующие категории:</p> <ol style="list-style-type: none"> 1. общедоступная и конфиденциальная; 2. ограниченного доступа и государственная тайна; 3. конфиденциальная информация и государственная тайна; 4. общедоступная и ограниченного доступа. | ограниченного доступа. |
| 23. | <p>Выделите верное определение термина "информация". Информация - это...</p> <ol style="list-style-type: none"> 1. сведения (сообщения, данные) в зависимости от формы их представления; 2. сведения (сообщения, данные) независимо от формы их представления, которые может воспринять человек; 3. сведения (сообщения, данные), доступ к которым ограничен; 4. сведения (сообщения, данные) независимо от формы их представления. | 4. сведения (сообщения, данные) независимо от формы их представления. |
| 24. | <p>Процессы, методы поиска, сбора, хранения, обработки, предоставления, распространения информации и способы осуществления таких процессов и методов это...</p> <ol style="list-style-type: none"> 1. информационная система; 2. автоматизированная система; 3. информационно - телекоммуникационная сеть; 4. информационная технология. | 4. информационная технология. |
| 25. | <p>Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств это...</p> <ol style="list-style-type: none"> 1. информационная технология; 2. автоматизированная система; 3. информационно - телекоммуникационная сеть; 4. информационная система. | 4. информационная система. |
| 26. | <p>Какая буква русского языка имеет самую максимальную частотность (результат в нижнем регистре)</p> | о |
| 27. | <p>Дано сообщение 10001_2 и ключ 00111_2 в двоичной системе счисления. Каков будет результат если применить алгоритм шифрования XOR</p> | 10110 |
| 28. | <p>Даны 2 простых числа 5 и 7 вычислите значение функции Эйлера от числа n, где $n=5*7=35$</p> | 24 |
| 29. | <p>Дан ряд простых чисел 2, 3, 5. В ответ впишите результат целочисленного деления числа 7 на указанный ряд. (В ответе числа указать подряд без пробелов и знаков препинания)</p> | 112 |
| 30. | <p>Для таблицы Виженера русского языка с какой буквой начнется вторая строка (ответ написать с нижнего регистра)</p> | б |

Составитель Кочеров Ю.Н.

Министерство науки и высшего образования Российской Федерации
Федеральное государственное автономное образовательное учреждение
высшего образования
«СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ»

**КРИТЕРИИ И ШКАЛЫ ОЦЕНИВАНИЯ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО
КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**

«5» (отлично): студент демонстрирует системные теоретические знания, владеет терминологией, делает аргументированные выводы и обобщения, приводит примеры, показывает свободное владение монологической речью и способность быстро реагировать на уточняющие вопросы.

«4» (хорошо): студент демонстрирует прочные теоретические знания, владеет терминологией, делает аргументированные выводы и обобщения, приводит примеры, показывает свободное владение монологической речью, но при этом делает несущественные ошибки, которые быстро исправляет самостоятельно или при незначительной коррекции преподавателем.

«3» (удовлетворительно): студент демонстрирует неглубокие теоретические знания, проявляет слабо сформированные навыки анализа явлений и процессов, недостаточное умение делать аргументированные выводы и приводить примеры, показывает недостаточно свободное владение монологической речью, терминологией, логичностью и последовательностью изложения, делает ошибки, которые может исправить только при коррекции преподавателем.

«2» (неудовлетворительно): студент демонстрирует незнание теоретических основ предмета, не умеет делать аргументированные выводы и приводить примеры, показывает слабое владение монологической речью, не владеет терминологией, проявляет отсутствие логичности и последовательностью изложения, делает ошибки, которые не может исправить даже при коррекции преподавателем, отказывается отвечать на занятии.