

Документ подписан простой электронной подписью

Информация о владельце:

ФИО: Алейник Станислав Николаевич

Должность: Ректор

Дата подписания:

Уникальный программный ключ:

5258223550ea7b6b23726a16078644b53d8986ab8255871f268f913a1351fae

**МИНИСТЕРСТВО СЕЛЬСКОГО ХОЗЯЙСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ АГРАРНЫЙ УНИВЕРСИТЕТ ИМЕНИ
В.Я.ГОРИНА»**

ПРОГРАММА

**вступительного испытания «Информационная безопасность» для
поступающих на направления подготовки бакалавриата 09.03.03
Прикладная информатика на базе профессионального образования**

п. Майский, 2021

Программа вступительного испытания по «Информационной безопасности» разработана для поступающих на направление подготовки бакалавриата 09.03.03- Прикладная информатика, составлена с учетом полученного предшествующего среднего профессионального образования.

Программа вступительного испытания разработана для приема на обучение по очной и заочной формам обучения на направления подготовки высшего образования.

ВВЕДЕНИЕ

На вступительном испытании по «Информационной безопасности» поступающий на направления подготовки высшего образования должен показать теоретические знания в профессиональной сфере и умения применять их в практической деятельности в пределах приведенной ниже программы.

Программа содержит перечень вопросов, позволяющих оценить уровень подготовки поступающего необходимого для освоения программы бакалавриата; критерии оценки; шкалу оценивания (100-балльная).

Общие положения для вступительного испытания по «Информационной безопасности» при приеме на направление подготовки бакалавриата 09.03.03 -Прикладная информатика следующие: поступающие пишут вступительное испытание в письменной форме.

Работа состоит из 2 теоретических вопросов и 2 ситуационных задач, требующих непосредственного письменного развернутого ответа и решения.

В программе приведен общий список литературы по разделам вступительного испытания. Список литературы носит рекомендательный характер. Программа вступительного испытания разработана на кафедре математики.

ОБЩИЕ ТРЕБОВАНИЯ К ПРОВЕДЕНИЮ ВСТУПИТЕЛЬНОГО ИСПЫТАНИЯ

Вступительное испытание проводится письменно, в очном формате. Допускается проведение вступительного испытания в дистанционном формате, при условии идентификации личности.

Шкала оценивания 100-балльная. На основе баллов, выставленных за выполнение всех заданий экзаменационной работы подсчитывается суммарное количество баллов, в том числе:

- за 1 теоретический вопрос максимум 25 баллов;
- за 1 ситуационную задачу максимум 25 баллов.

На выполнение всей экзаменационной работы с учетом заполнения бланков и проверки работы экзаменуемым отводится 240 минут.

Письменная работа включает в себя перечень вопросов, позволяющих оценить уровень знаний абитуриента по основным темам вступительного испытания. Абитуриенты, получившие баллы ниже установленного правилами приема минимального порога, не допускаются к участию в конкурсе.

СОДЕРЖАНИЕ ТЕМ

1. Составляющие, уровни обеспечения и угрозы ИБ
2. Вирусы и удаленные угрозы в сетях
3. Принципы и методы защиты в вычислительных сетях

ПЕРЕЧЕНЬ ТЕОРИТИЧЕСКИХ ВОПРОСОВ К ВСТУПИТЕЛЬНОМУ ИСПЫТАНИЮ

1. Понятие информационной безопасности.
2. Составляющие информационной безопасности.
3. Уровни информационной безопасности.
4. Угрозы информационной безопасности.
5. Ключевые принципы информационной безопасности.
6. Понятие доступности информации.
7. Понятие целостности информации.
8. Понятие конфиденциальности информации.
9. Нормативные документы в области информационной безопасности.
10. Органы, обеспечивающие информационную безопасность.
11. Организационно-технические и режимные меры и методы
12. Начальное форматирование диска.
13. Дисковые утилиты
14. Проверка диска.
15. Очистка диска.
16. Дефрагментация диска.
17. Проверка и очистка реестра.
18. Антивирусные средства.
19. Файерволлы.
20. Как определить физический адрес компьютера?
21. Как определить внутренний IP адрес компьютера?
22. Как определить внешний IP адрес компьютера?
23. Как определить сетевое окружение компьютера?
24. Как проверить защищенность данных компьютера в сетевом окружении?
25. Как определить доступность данных вашего компьютера для сетевого окружения?
26. Как определить владельца информационного ресурса?
27. Как узнать оператора хостинга информационного ресурса?
28. Как определить, используется ли ресурсом защищенный протокол передачи данных?
29. Диагностика компьютера.
30. Диагностика подключения к сети Интернет.
31. Диагностика сайта.

32. Сетевые службы диагностики сайта.
33. Удаленные сетевые атаки.
34. Сниффинг.
35. Спуффинг.
36. Флудинг.
37. Фишинг.
38. Вишинг.
39. Смишинг.
40. Mailbombing.
41. Фарминг.
42. Настройка браузера.
43. История браузера. Очистка.
44. Кукисы. Применение. Ограничения.
45. Индикаторы безопасности сайтов в ИПС.
46. Применение http и https. В чем разница с точки зрения безопасности?
47. Прокси и анонимайзеры. Есть ли выигрыш в безопасности?
48. Оцените пользу для обеспечения безопасности «луковичного сервиса».
49. Что делать, если компьютер не реагирует на действия пользователя?
50. Как вызвать диспетчер задач?

ПЕРЕЧЕНЬ СИТУАЦИОННЫХ ЗАДАЧ К ВСТУПИТЕЛЬНОМУ ИСПЫТАНИЮ

1. Определите распределение памяти по дискам.
2. Оцените безопасность распределения памяти по дискам.
3. Выполните проверку диска на ошибки.
4. Составьте отчет проверки диска на ошибки.
5. Выполните очистку диска.
6. Составьте отчет очистки диска.
7. Выполните дефрагментацию диска.
8. Составьте отчет дефрагментации диска.
9. Выполните проверку и очистку реестра.
10. Составьте отчет проверки реестра
11. Составьте отчет очистки реестра
12. Определите антивирус, используемый на данном компьютере.
13. Определите фаерволл, используемый на данном компьютере..
14. Определите физический адрес компьютера.
15. Определите внутренний IP адрес компьютера.
16. Определите внешний IP адрес компьютера.
17. Определите сетевое окружение компьютера
18. Дайте характеристику сетевого окружения компьютера.
19. Оцените защищенность данных компьютера в сетевом окружении.
20. Определите доступность данных вашего компьютера для сетевого окружения.
21. Определите владельца указанного информационного ресурса.
22. Определите оператора хостинга указанного информационного ресурса.

23. Определите, используется ли ресурсом защищенный протокол передачи данных.
24. Проведите диагностику компьютера
25. Определите характеристики, версии ПО компьютера
26. Проведите диагностику подключения компьютера к сети Интернет.
27. Выполните диагностику указанного сайта.
28. Определите настройка браузера компьютера.
29. Зафиксируйте настройка браузера компьютера
30. Произведите очистку истории браузера.
31. Сделайте отчет очистки истории браузера.
32. Определите протокол передачи гипертекста, используемый указанным сайтом.
33. Вызовите диспетчер задач, сделайте отчет по использованию вычислительной мощности компьютера процессами.
34. Вызовите диспетчер задач, определите процесс, использующий максимальную долю вычислительной мощности компьютера.
35. Запустите диспетчер задач, на вкладке «быстродействие» определите и оцените хронологию загрузки ЦП и использования физической памяти.
36. Оцените защищенность компьютера вашего рабочего места от вирусов
37. Оцените защищенность данных на компьютерах вашего сетевого окружения
38. Оцените защищенность данных на серверах сети. Дайте оценку полученным результатам.
39. Оцените эффективность и безопасность работы компьютера вашего рабочего места.
40. Дайте оценку полученным результатам.
41. Произведите оценку доступности компьютера вашего рабочего места для сетевых атак .
42. Дайте оценку полученным результатам.
43. Произведите оценку открытости для сетевых атак заданного сайта.
44. Узнайте IP - адрес, владельца сайта.
45. Узнайте дату регистрацию домена.
46. Узнайте оплату домена.
47. Узнайте используемое ПО (CMS). Дайте оценку полученным результатам.
48. Произведите определение настроек браузера вашего компьютера, влияющих на безопасности работы в сети Интернет
49. При включении компьютера, находящегося в корпоративной сети, вы обнаружили, что диск D не содержит информации, которая там была. Видимо, вирус сделал все объекты скрытыми. У вас нет прав администратора. Можно ли решить проблему без вызова инженера? Опишите ваши действия.
50. Пользователь заметил, что ПК стал выполнять операции, команды, которые им не отдавались, перезагружаться, «тормозить». Перечислите возможные причины. Составьте список действий, которые должен последовательно произвести пользователь.

РЕКОМЕНДУЕМАЯ ЛИТЕРАТУРА, ИНТЕРНЕТ-ИСТОЧНИКИ

1. Партыка, Т.Л. Информационная безопасность: Учебное пособие [Электронный ресурс]/ Т.Л. Партыка, И.И. Попов. - 5-е изд., перераб. и доп. - М.: Форум: НИЦ ИНФРА-М, 2014. - 432 с.

2. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие [Электронный ресурс]/ В.Ф. Шаньгин. - М.: ИД ФОРУМ: НИЦ ИНФРА-М, 2014. - 416

3. Миронов, А.Л. Информационная безопасность: Учебное пособие[Текст]/ А.Л. Миронов // Изд. Белгородского ГАУ, 2014. – 46 с.

КРИТЕРИИ ОЦЕНКИ ЗНАНИЙ ЗА ОДНО ТЕОРЕТИЧЕСКОЕ ЗАДАНИЕ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Оценка	Критерии
25 баллов	систематизированный, глубокий, полный ответ на все вопросы экзаменационного билета; точное использование научной терминологии, стилистически грамотное, логически правильное изложение ответов на вопросы; умение обосновать излагаемый материал практическими примерами; умение дать системную связь теоретического материала с практической деятельностью в современных условиях.
20 баллов	систематизированный, полный, достаточно глубокий ответ на экзаменационные вопросы; знание и умелое использование научной терминологии, логическое построение ответа; умение иллюстрировать ответ конкретными практическими примерами.
15 баллов	достаточно полные ответы на вопросы экзаменационного билета; понимание и умение пользоваться терминологией; умение использовать определенный материал; умение показать связь с практикой.
10 баллов	достаточный объем знаний в рамках экзаменационного билета; понимание основной терминологии.
5 баллов	отрывочные знания вопросов, слабое представление об их содержании; неумение обосновывать практическим примером теоретические положения.
0 баллов	отсутствие знаний и компетенций в рамках экзаменационного вопроса, незнание сущности основных понятий и их содержания; отказ от ответа из-за незнания содержания вопросов билета.

КРИТЕРИИ ОЦЕНКИ ЗНАНИЙ ЗА ОДНУ СИТУАЦИОННУЮ ЗАДАЧУ ЭКЗАМЕНАЦИОННОГО БИЛЕТА

Оценка	Критерии
25 баллов	ответ на вопрос задачи дан правильный. Объяснение хода ее решения подробное, последовательное, грамотное, с необходимыми обоснованиями, схематическими изображениями и графическими демонстрациями.
20 баллов	ответ на вопрос задачи дан правильный. Объяснение хода ее решения подробное, но недостаточно логичное, с единичными

	ошибками в деталях, некоторыми затруднениями в теоретическом обосновании, в схематических изображениях и демонстрациях.
15 баллов	ответ на вопрос задачи дан правильный. Объяснение хода ее решения недостаточно полное, непоследовательное, с незначительными ошибками, слабым теоретическим обоснованием, без схематических изображений и графических демонстраций
10 баллов	ответ на вопрос задачи дан правильный. Объяснение хода ее решения неполное, нелогичное, непоследовательное, с грубыми ошибками, слабым обоснованием, без схематических изображений и графических демонстраций.
5 баллов	ответ на вопрос задачи дан не верный. Объяснение хода решение ситуационной задачи дано неполное, непоследовательное, с грубыми ошибками, без схематических изображений и графических демонстраций.
0 баллов	решение ситуационной задачи отсутствует.

**ДЕМОНСТРАЦИОННЫЙ ВАРИАНТ
ЭКЗАМЕНАЦИОННОГО БИЛЕТА**

Федеральное государственное бюджетное образовательное учреждение высшего образования «Белгородский государственный аграрный университет имени В. Я. Горина»

вступительные испытания по «Информационной безопасности» для направления подготовки 09.03.03- Прикладная информатика при приеме на обучение на 2022-2023 учебный год

УТВЕРЖДАЮ:
Зам. председателя приемной комиссии
_____ **Клостер Н.И.**
от «29» октября 2021 г.

Билет № 1

1. Понятие целостности информации.
2. Диагностика подключения к сети Интернет
3. Произведите определение настроек браузера вашего компьютера, влияющих на безопасности работы в сети Интернет
4. Пользователь заметил, что ПК стал выполнять операции, команды, которые им не отдавались, перезагружаться, «тормозить». Перечислите возможные причины. Составьте список действий, которые должен последовательно произвести пользователь

Составитель

Миронов А.Л.