Федеральное государственное бюджетное образовательное учреждение высшего образования «Российский государственный университет правосудия»

(ФГБПРУВО «РГУП»)

Приложение к п. 3

Рабочей программы: «Основы информационной безопасности для кадетских классов» (10-11кл.)

**Демонстрационный вариант**

**«Основы информационной безопасности для кадетских классов»**

**(10 класс)**

Автор-составитель: Быков Антон Олегович,

директор центра обезличивания персональных данных, член ТК 164 «Искусственный интеллект», руководитель

направления ФГУ НИИ «Восход, преподаватель МГИМО

Рецензент: Шабанин Олег Васильевич,

доцент кафедры математического анализа и теории вероятностей

Института криптографии, связи и информатики Академии ФСБ России,

кандидат физико – математических наук.

Москва – 2023

**1. Пояснительная записка**

Настоящий демонстрационный вариант контрольно-измерительных материалов устанавливает перечень заданий для оценки результатов обучения кадет, обучающихся по городскому образовательному проекту «Кадетский класс в московской школе».

Контрольно-измерительные материалы предназначены для преподавателей, реализующих программу «Основы информационной безопасности для кадетских классов», 10 класс, разработаны в ФГБПРУВО «РГУП» с учётом выбранного профиля МВД/МИНЮСТ предпрофессиональной подготовки обучающихся проекта предпрофессионального образования «Кадетский класс в московской школе» в соответствии с:

Приказом Министерства образования и науки РФ 17.05.2012 № 413 (ред. от 12.08.2022 г.) «Об утверждении Федерального государственного образовательного стандарта среднего общего образования»;

Приказом Министерства просвещения РФ от 27.07.2022 № 629 «Об утверждении Порядка организации и осуществления образовательной деятельности по дополнительным общеобразовательным программам»;

Техническим заданием на оказание услуг по организации и проведению предпрофессионального экзамена для обучающихся образовательных организаций - участников образовательного проекта «Кадетский класс в московской школе».

При ознакомлении с демонстрационным вариантом контрольно-измерительных материалов (КИМ) – демоверсия – для оценки результатов обучения кадет, обучающихся по образовательному проекту «Кадетский класс в московской школе» следует иметь в виду, что задания, включённые в него, содержат конкретные примеры для проверки знаний по рабочей программе за 10 класс «Основы информационной безопасности для кадетских классов».

***Назначение демонстрационного варианта:***

Заключается в том, чтобы дать возможность любому обучающемуся составить представление о структуре будущих вариантов ким, количестве заданий, об их форме, уровне сложности.

Приведённые критерии оценки выполнения задания, включенного в демонстрационный вариант ким, дают представление о требованиях к полноте и правильности ответа. Эти сведения позволят выпускникам выработать стратегию подготовки к тестированию.

***Цель и задачи демонстрационного варианта контрольно-измерительных материалов:***

*Цель контрольно-измерительных материалов:*

Диагностика степени усвоения программы обучающимися.

*Задачи демонстрационного варианта контрольно-измерительных материалов*:

Способствовать выявлению степени усвоения программы обучающимися;

Выявить пробелы в знаниях обучающихся и своевременно их корректировать;

Успешно подготовиться к итоговому тестированию с учетом выявленных пробелов в знаниях обучающихся.

***Формы демонстрационного варианта контрольно-измерительных материалов:***

Демонстрационный вариант контрольно-измерительных материалов рабочей программы «Основа информационной безопасности для кадетских классов» представляют собой совокупность тестов.

Тест - это система стандартизированных вопросов (заданий) позволяющих автоматизировать процедуру измерения уровня знаний и умений обучающихся.

Тестовые задания могут иметь различные структуры, в том числе: с одним или несколькими вариантами верного ответа, содержать открытый вопрос, задание на сопоставление, задание на установление верной последовательности.

Тест обучающимся может быть представлен как на бумажном носителе, так и с применением информационно-телекоммуникационных технологий в информационной образовательной среде организации или с использованием доступных инструментов тестирования в сети Интернет.

О проведении теста, его формы, а также раздел (темы) дисциплины, выносимых на тестирование, до сведения обучающихся доводит преподаватель.

Обучающемуся предлагается ответить на 20 тестовых вопросов, охватывающих основные аспекты дисциплины «Основы информационной безопасности для кадетских классов» согласно изученным за 10 класс по дисциплине темам.

**3.   Тест демонстрационного варианта**

1. Что такое информационная безопасность?

а) Процесс защиты устройств от несанкционированного доступа, использования, изменения, повреждения, уничтожения и других угроз.

б) Процесс защиты сетей от несанкционированного доступа, использования, изменения, повреждения, уничтожения и других угроз.

в) Процесс защиты информационных технологий, устройств, сетей и данных от несанкционированного доступа, использования, изменения, повреждения, уничтожения и других угроз.

Ответ: в)

2. Что такое конфиденциальность информации?

а) Свойство информации, которое означает, что только авторизованный пользователь или группа пользователей имеют доступ к этой информации.

б) Свойство информации, которое означает, что информация доступна для авторизованных пользователей в тот момент, когда это необходимо.

в) Свойство информации, которое означает, что информация не должна быть модифицирована, уничтожена или изменена без авторизации.

Ответ: а)

3. Что такое доступность информации?

а) Свойство информации, которое означает, что только авторизованный пользователь или группа пользователей имеют доступ к этой информации.

б) Свойство информации, которое означает, что информация доступна для авторизованных пользователей в тот момент, когда это необходимо.

в) Свойство информации, которое означает, что информация не должна быть модифицирована, уничтожена или изменена без авторизации.

Ответ: б)

4. Что такое целостность информации?

а) Свойство информации, которое означает, что только авторизованный пользователь или группа пользователей имеют доступ к этой информации.

б) Свойство информации, которое означает, что информация доступна для авторизованных пользователей в тот момент, когда это необходимо.

в) Свойство информации, которое означает, что информация не должна быть модифицирована, уничтожена или изменена без авторизации.

Ответ: в)

5. Что такое интернет вещей?

а) Вирус, который заражает компьютеры.

б) Это система взаимосвязанных вычислительных устройств, которые могут собирать и передавать данные по беспроводной сети без участия человека.

в) Раздел интернета, в котором продаются вещи.

Ответ: б)

6. Что такое нормативный правовой акт?

а) Это официальный документ, принятый (изданный) в определенной форме правотворческим органом в пределах его компетенции и направленный на установление, изменение и отмену правовых норм.

б) Это документ, принятый (изданный) в определенной форме правотворческим органом в пределах его компетенции и направленный на установление, изменение и отмену правовых норм.

в) Это официальный документ, принятый (изданный) и направленный на установление, изменение и отмену правовых норм.

Ответ: а)

7. Что такое государственная тайна?

а) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

б) Защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности.

в) Защищаемые государством сведения в области его военной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации.

Ответ: а)

8. Что такое технические средства противодействия угрозам?

а) Программно-аппаратный комплекс, позволяющий ограничивать доступ к информации, распространение которой запрещено на территории Российской Федерации.

б) Программно-аппаратный комплекс, позволяющий ограничивать доступ к информации, распространение которой разрешено на территории Российской Федерации.

в) Программный комплекс, позволяющий ограничивать доступ к информации, распространение которой запрещено на территории Российской Федерации.

Ответ: а)

9. Какие существуют внутренние угрозы информационной безопасности?

а) Ошибки или небрежности в действиях сотрудников.

б) Кибератаки.

в) Все вышеперечисленное.

Ответ: а)

10. Какие существуют внешние угрозы информационной безопасности?

а) Вирусы и хакеры.

б) Кибератаки.

в) Все вышеперечисленное.

Ответ: в)

**11.** Авторизация позволяет контролировать…

а) Кто может получить доступ к информации и в каких случаях.

б) Целостность информации.

в) Защиту от вирусов.

Ответ: а)

12. Ключ шифрования – это:

а) Использование информации для изменения поведения людей.

б) Набор символов, нужных для получения доступа к информации.

в) Набор параметров, используемых при шифровании и дешифровании информации.

Ответ: в)

13. Какие существуют угрозы информационной безопасности, связанные с шифрованием?

а) Компрометация ключа.

б) Взлом или атака посредством перехвата паролей.

в) Все вышеперечисленное.

Ответ: в)

14. Внешние нарушители – это:

а) Нарушители, не имеющие прав доступа в контролируемую зону и (или) полномочий по доступу к информационным ресурсам.

б) Нарушители, имеющие права доступа в контролируемую зону и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации.

в) Нарушители, не имеющие прав доступа в контролируемую зону и (или) полномочий по доступу к информационным ресурсам и компонентам систем и сетей, требующим авторизации.

Ответ: в)

15. Внутренние нарушитель – это:

а) Нарушители, имеющие права доступа в контролируемую зону и (или) полномочий по доступу к информационным ресурсам.

б) Нарушители, не имеющие прав доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей.

в) Нарушители, имеющие права доступа в контролируемую (охраняемую) зону (территорию) и (или) полномочия по автоматизированному доступу к информационным ресурсам и компонентам систем и сетей.

Ответ: в)

16. Кибератака – это:

а) Специально организованный процесс, при котором злоумышленники пытаются получить несанкционированный доступ к информационным ресурсам цели.

б) Взлом информационных систем.

в) Выведение из строя сетей противника.

Ответ: а)

17. Гриф секретно относится к информации:

а) раскрытие которой может привести к серьезному ущербу для государства.

б) раскрытие которой может привести к опасности для существования государства или нанести тяжелый ущерб его безопасности.

в) раскрытие которой может привести к глобальной опасности для национальной безопасности России и ее народа, а также международной безопасности.

Ответ: а)

18. ISO/IEC 27001– это:

а) международный стандарт, который устанавливает требования к системам управления информационной безопасностью.

б) Интернет протокол.

в) Вид уязвимости.

Ответ: а)

19. Модель нарушителя – это:

а) Набор предположений об одном или нескольких возможных нарушителях информационной безопасности, их квалификации, их технических и материальных средствах и т. д.

б) Набор предположений об одном или нескольких возможных нарушителях Уголовного Кодекса РФ, их квалификации, их технических и материальных средствах и т. д.

в) Ничего из вышеперечисленного.

Ответ: а)

20) Что такое несанкционированный доступ?

а) Процесс, при котором злоумышленники получают доступ к информации, которая не предназначена для них.

б) Процесс, при котором злоумышленники получают доступ к информации, которая предназначена для них.

в) Использование кибератак для получения доступа к информации.

Ответ: а)

**3.2** Время выполнения задания – 45 минут.