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.)

**СБОРНИК**

**Контрольно-измерительных материалов**

**(КИМы)**

**(1-е полугодие 10 класса)**

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**

Настоящие контрольно-измерительные материалы устанавливают перечень заданий для оценки результатов обучения кадетов программе «Основы информационной безопасности для кадетских классов» в рамках городского проекта «Кадетский класс в московской школе».

Контрольно-измерительные материалы предназначены для педагогов, реализующих программу «Основы информационной безопасности для кадетских классов», разработаны в ФГБПРУВО «РГУП» с учётом выбранного профиля 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».

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

*Целями контрольно-измерительных материалов*являются:

контроль усвоения предметных результатов образования;

установление их соответствия планируемым результатам освоения основной дополнительной общеобразовательной общеразвивающей программы «Основы информационной безопасности для кадетских классов» базового уровня образования.

*Задачи контрольно-измерительных материалов*:

обеспечение процесса оценки качества освоения дополнительной общеобразовательной общеразвивающей программы «Основы информационной безопасности для кадетских классов» современным инструментарием;

обеспечение единого подхода к оценке качества образования;

определение эффективности организации образовательной деятельности в рамках проведения городского проекта «Кадетский класс в московской школе»;

выявление пробелов в знаниях, обучающихся и своевременная их корректировка.

***Формы контрольно-измерительных материалов:***

Контрольно-измерительные материалы рабочей программы «Основы информационной безопасности для кадетских классов» представляют собой совокупность тестового и контрольных заданий.

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.

КИМы состоят из 3 вариантов по 20 вопросов, включающие вопросы по изученным темам в первом полугодии 10 класса:

|  |  |
| --- | --- |
| 1 | Основы информационной безопасности |
| 1.1 | Введение в информационную безопасность. Основные понятия. |
| 1.2 | Угрозы в информационной безопасности. Основные виды. |
| 1.3 | Технические средства защиты информации и основные каналы утечки. |
| 1.4 | Защита информационных систем. Основные методы и средства. |

*Критерии оценивания:*

Оценки результатов тестирования можно соотнести с общепринятой пятибалльной шкалой:

«неудовлетворительно» – правильно ответил на 5 и менее тестовых вопросов из 20 тестовых вопросов проводимой аттестации;

«удовлетворительно» – правильно ответил на 6-10 тестовых вопросов из 20 тестовых вопросов проводимой аттестации;

«хорошо» – правильно ответил на 11-15 тестовых вопросов из 20 тестовых вопросов проводимой аттестации;

«отлично» – правильно ответил на 16-20 тестовых вопросов из 20 тестовых вопросов проводимой аттестации.

Рекомендуется проведение работы над ошибками.

*Практическая значимость* контрольно-измерительных материалов:

Разработанные контрольно-измерительные материалы способствуют подготовке к предпрофессиональному экзамену в рамках городского проекта «Кадетский класс в московской школе» по элективной программе «Основы информационной безопасности для кадетских классов» 10-11 классов.

# 2. Кодификатор элементов содержания и требований к уровню подготовки обучающихся для проведения промежуточной аттестации по «Основы информационной безопасности для кадетских классов».

|  |  |  |  |
| --- | --- | --- | --- |
| **Код контроли- руемого**  **требования** | **Требования к результатам освоения дополнительной общеобразовательной общеразвивающей программы, проверяемые контрольными заданиями** | | |
| **Компонент ожидаемых результатов освоения дополнительной общеобразовательной общеразвивающей программы** | **Рабочая программа** | |
| *базовый уровень* | *углублённый уровень* |
| 1 | 2 | 3 | 4 |
| ***1*** | ***Знать*** |  |  |
| 1.1 | Введение в информационную безопасность. Основные понятия. | Основные понятия информационной безопасности. Определения и термины. Рассмотрение информационной безопасности как отдельной области знаний. | Не предусмотрен |
| 1.2 | Угрозы в информационной безопасности. Основные виды. | Понятие угрозы в контексте информационной безопасности. Основные виды угроз и сферы их возникновения. Известные модели распространения угроз. Модель нарушителя. | Не предусмотрен |
| 1.3 | Технические средства защиты информации и основные каналы утечки. | Понятие утечки информации. Виды утечек по воздействию с устройствами. Понятие защиты информации с помощью технических средств. Каналы передачи данных. | Не предусмотрен |
| 1.4 | Защита информационных систем. Основные методы и средства. | Понятие защиты информационных систем. Комплексный подход к безопасности информационных систем. Методы противодействия нарушителям. Межсетевые экраны, антивирусы и прочие программные средства защиты информационных систем. | Не предусмотрен |

**3. Спецификация контрольных измерительных материалов**

**3.1 Тест Вариант № 1**

1. Что такое информационная безопасность?

а) защита технических устройств от повреждений

б) защита информации от несанкционированного доступа, копирования или изменения

в) защита здоровья при работе за компьютером

2. Какие виды информации могут быть защищены?

а) только коммерческая информация

б) только персональные данные

в) любые виды информации

3. Что такое угрозы в информационной безопасности?

а) возможные ситуации, которые могут повредить информационным процессам и системам

б) технические средства защиты информации

в) способы безопасного соединения с интернетом

4. Какие виды угроз в информационной безопасности существуют?

а) только физические угрозы

б) только технические угрозы

в) физические, технические и социально-психологические

5. Что такое социальная инженерия?

а) технический метод защиты информации

б) техника взлома с помощью манипуляций человеком

в) защита от вирусов

6. Что такое шифрование?

а) защита информации при помощи паролей

б) преобразование информации в нечитаемый для третьих лиц вид

в) аппаратное обеспечение безопасности информации

7. Какие технические средства защиты информации существуют?

а) только аппаратное обеспечение

б) только программное обеспечение

в) аппаратное и программное обеспечение

8. Какие каналы утечки информации существуют?

а) только через интернет

б) только по внутренней сети организации

в) внутренние и внешние

9. Какие методы защиты информационных систем существуют?

а) только программные методы

б) только аппаратные методы

в) программные и аппаратные методы

10. Что такое аутентификация?

а) процедура проверки подлинности пользователя

б) проверка наличия антивирусной программы на компьютере

в) проверка системы на наличие уязвимостей

**11. К основным принципам информационной безопасности относятся:**

а) Конфиденциальность, доступность, целостность

б) Своевременность, логичность, единообразие

в) Первичность, недоступность, осведомленность

**12. Основными субъектами информационной безопасности являются:**

а) руководители, менеджеры, администраторы компаний

б) владельцы и пользователи информации

в) сетевые базы данных, фаерволлы

**13. К основным функциям системы безопасности можно отнести все перечисленное:**

а) Установление авторизации и аутентификации, аудит системы, выявление рисков

б) Установка новых офисных приложений, смена хостинг-компании

в) Внедрение аутентификации, проверки контактных данных пользователей

**14. Что такое антивирусное программное обеспечение?**

**а) Программа для создания резервных копий данных**

**б) Программа для удаления нежелательного почтового спам-письма**

**в) Программный продукт, предназначенный для защиты операционной системы от вредоносных программ**

**15. Принципом политики информационной безопасности является принцип:**

а) Невозможности миновать защитные средства сети (системы)

б) Усиления основного звена сети, системы

в) Полного блокирования доступа при возникновении рисков

**16. Принципом политики информационной безопасности является принцип:**

а) Усиления защищенности самого незащищенного звена сети (системы)

б) Перехода в безопасное состояние работы сети, системы

в) Полного доступа пользователей ко всем ресурсам сети, системы

**17. Какие виды угроз могут возникать для информационной безопасности?**

**а) Только хакерские атаки**

**б) Все, что может привести к утечке или повреждению данных (взлом, вирусы, ошибки персонала и т.д.)**

**в) Только физическое повреждение оборудования**

**18. Что такое пароль?**

**а) Способ зашифровывания данных на жестком диске**

**б) Уникальный код доступа к системам и данным пользователя**

**в) Название программы для удаления вредоносных файлов**

**19. Что такое двухфакторная аутентификация?**

**а) Аутентификация по голосу**

**б) Аутентификация с помощью двух разных методов (например, пароль и SMS-код)**

**в) Аутентификация с помощью одного метода**

**20. Что такое вирус?**

**а) Программа для защиты компьютера от хакерских атак**

**б) Вредоносная программа, которая может повредить файлы на компьютере или украсть данные пользователя**

**в) Способ передачи данных между несколькими устройствами**

**3.2 Тест Вариант № 2**

1. Что такое информационная безопасность?

а) защита технических устройств от повреждений

б) защита информации от несанкционированного доступа, копирования или изменения

в) защита здоровья при работе за компьютером

2. Какие виды информации могут быть защищены?

а) только коммерческая информация

б) только персональные данные

в) любые виды информации

3. Что такое угрозы в информационной безопасности?

а) возможные ситуации, которые могут повредить информационным процессам и системам

б) технические средства защиты информации

в) способы безопасного соединения с интернетом

4. Какие виды угроз в информационной безопасности существуют?

а) только физические угрозы

б) только технические угрозы

в) физические, технические и социально-психологические

5. Что такое социальная инженерия?

а) технический метод защиты информации

б) техника взлома с помощью манипуляций человеком

в) защита от вирусов

6. Что такое шифрование?

а) защита информации при помощи паролей

б) преобразование информации в нечитаемый для третьих лиц вид

в) аппаратное обеспечение безопасности информации

7. Какие технические средства защиты информации существуют?

а) только аппаратное обеспечение

б) только программное обеспечение

в) аппаратное и программное обеспечение

8. Какие каналы утечки информации существуют?

а) только через интернет

б) только по внутренней сети организации

в) внутренние и внешние

9. Какие методы защиты информационных систем существуют?

а) только программные методы

б) только аппаратные методы

в) программные и аппаратные методы

10. Что такое аутентификация?

а) процедура проверки подлинности пользователя

б) проверка наличия антивирусной программы на компьютере

в) проверка системы на наличие уязвимостей

11. Что такое бэкап?

а) процесс сохранения данных в облаке

б) копия данных с целью их восстановления при потере данных

в) удаление данных из системы

12. Какие программы наиболее эффективно защищают от вирусов?

а) браузеры

б) медиаплееры

в) антивирусные программы

13. Что такое политики информационной безопасности?

а) сборник правил и рекомендаций для защиты информации

б) стратегия по защите компании

в) разработка инфраструктуры для защиты информации

14. Какие методы используются для защиты информации?

а) использование резервного копирования

б) использование антивирусных программ

в) использование антивирусных программ, защита паролей и шифрование данных, использование резервного копирования

15. Что такое DDoS-атака?

а) атака на базы данных

б) атака на компьютер с целью удаления данных

в) атака на сеть с целью ее перегрузки

16. Что такое защита от перехвата?

а) защита от повреждения данных

б) защита от несанкционированного доступа к данным

в) все вышесказанное

17. Как называются программы, которые собирают информацию о пользователе без его ведома?

а) трояны

б) шпионские программы

в) вредоносные программы

12. Что такое брандмауэр?

а) программа для защиты компьютерной системы от вирусов

б) программа для мониторинга и блокировки сетевых соединений

в) программа для повышения производительности компьютера

19. Какие методы используются для защиты компьютерных сетей?

а) использование паролей и шифрования

б) использование сетевых экранов

в) все вышесказанное

20. Что такое многофакторная аутентификация?

а) проверка пароля и логина

б) проверка персональных данных

в) использование нескольких методов проверки личности

**3.3 Тест Вариант № 3**

1. Что такое информационная безопасность?

а) Защита от вирусов

б) Защита информации от несанкционированного доступа и дальнейшего использования

в) Оптимизация работы компьютерной сети

2. Какие вопросы, из перечисленных ниже, рассматриваются в информационной безопасности?

а) Взлом пароля пользователя системы

б) Шифрование жесткого диска

в) Все вышеперечисленные

3. Что такое аутентификация?

а) Процесс проверки подлинности пользователя или устройства

б) Программный продукт, который защищает компьютерную сеть от злоумышленников.

в) Системный вызов операционной системы, используемый для создания новых процессов.

4. Что такое бэкап?

а) Создание резервной копии данных

б) Удаление всех файлов с компьютера

в) Программа для защиты от вирусов

**5. К правовым методам, обеспечивающим информационную безопасность, относятся:**

а) Разработка аппаратных средств обеспечения безопасности данных

б) Разработка и установка во всех компьютерных сетях журналов учета действий

в) Разработка и конкретизация правовых актов обеспечения безопасности

**6. Основными источниками угроз информационной безопасности являются:**

а) Хищение жестких дисков, подключение к сети

б) Перехват данных, хищение данных, изменение архитектуры системы

в) Хищение данных, подкуп системных администраторов, нарушение регламента работы

**7. Виды конфиденциальной информации:**

а) Персональная(личная), коммерческая, государственная

б) Клиентская, серверная, сетевая

в) Локальная, глобальная, смешанная

**8. Цели информационной безопасности – своевременное обнаружение, предупреждение:**

а) Несанкционированного доступа, воздействия в сети

б) Утечек данных в организации

в) Чрезвычайных ситуаций

**9. Основные объекты информационной безопасности компьютерных систем:**

а) Компьютерные сети, базы данных

б) Психологическое состояние пользователей

в) Бизнес-ориентированные, коммерческие системы

**10. Основными рисками информационной безопасности являются:**

а) Искажение, уменьшение объема информации

б) Техническое вмешательство, выведение из строя оборудования сети

в) Потеря, искажение, утечка информации

**11. Основными субъектами информационной безопасности являются:**

а) руководители, менеджеры, администраторы компаний

б) владельцы и пользователи информации

в) сетевые базы данных, фаерволлы

12. Какие программы наиболее эффективно защищают от вирусов?

а) браузеры

б) медиаплееры

в) антивирусные программы

13. Что такое политики информационной безопасности?

а) сборник правил и рекомендаций для защиты информации

б) стратегия по защите компании

в) разработка инфраструктуры для защиты информации

14. Какие методы используются для защиты информации?

а) использование резервного копирования

б) использование антивирусных программ

в) использование антивирусных программ, защита паролей и шифрование данных, использование резервного копирования

15. Что такое DDoS-атака?

а) атака на базы данных

б) атака на компьютер с целью удаления данных

в) атака на сеть с целью ее перегрузки

16. Что такое защита от перехвата?

а) защита от повреждения данных

б) защита от несанкционированного доступа к данным

в) все вышесказанное

17. Как называются программы, которые собирают информацию о пользователе без его ведома?

а) трояны

б) шпионские программы

в) вредоносные программы

18. Что такое брандмауэр?

а) программа для защиты компьютерной системы от вирусов

б) программа для мониторинга и блокировки сетевых соединений

в) программа для повышения производительности компьютера

19. Какие методы используются для защиты компьютерных сетей?

а) использование паролей и шифрования

б) использование сетевых экранов

в) все вышесказанное

20. Что такое многофакторная аутентификация?

а) проверка пароля и логина

б) проверка персональных данных

в) использование нескольких методов проверки личности

**3.4 Проверяемые элементы, баллы, время выполнения задания**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| № | Проверяемые элементы содержания | Коды проверяемых элементов  содержания (по кодификатору) | Уровень сложности задания | Макс. балл  за  выполнени е задания | Примерное время  выполнения задания  (мин.) |
| 1 | Тест | 1.1 – 1.4 | Б | 5 | 10 |