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

(ФГБПРУВО «РГУП»)

Приложение к п. 3

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

**СБОРНИК**

**Контрольно-измерительных материалов**

**(КИМы)**

**(1-е полугодие 11 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» для 10-11 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 11 класса:

|  |  |
| --- | --- |
| 1 | Информационная безопасность в сети Интернет и «цифровая гигиена» |
| 1.1 | Публикация персональной информации. Приватность и конфиденциальность в сети. |
| 1.2 | Фишинг. Варианты воздействия и способы защиты. |
| 1.3 | Социальная инженерия. Правила безопасности при общении в сети. |
| 1.4 | Безопасность аккаунтов в сети. Совершение покупок онлайн. |

*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» для 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 | Публикация персональной информации. Приватность и конфиденциальность в сети. | Понятие безопасности в сети Интернет. Понятие цифровой гигиены. Пример безопасного поведения в сети интернет. Понятие персональной информации. Открытая и приватная информация. Понятие конфиденциальности. | Не предусмотрен |
| 1.2 | Фишинг. Варианты воздействия и способы защиты. | Понятие фишинга. Механизм работы фишинга. Примеры применения и способы защиты. | Не предусмотрен |
| 1.3 | Социальная инженерия. Правила безопасности при общении в сети. | Понятие социальной инженерии. Общение в сети интернет. Сферы применения и методики воздействия. Способы противодействия социальной инженерии.  информационной безопасности. Методы оценки рисков безопасности информационной системы. | Не предусмотрен |
| 1.4 | Безопасность аккаунтов в сети. Совершение покупок онлайн. | Методика безопасного создания и администрирования аккаунтов в сети Интернет. Способы усиления защиты аккаунтов. Покупки онлайн. Меры предосторожности при совершении покупок онлайн. | Не предусмотрен |

**3. Спецификация контрольных измерительных материалов**

**3.1 Тест Вариант № 1»**

1. Что такое открытая информация?

а) Информация, которая доступна только для определенных лиц

б) Информация, которая должна быть защищена

в) Информация, которая может быть свободно доступна всем

2. Что такое приватная информация?

а) Информация, которая доступна только для определенных лиц

б) Информация, которая должна быть защищена

в) Информация, которая может быть свободно доступна всем

3. Что такое цифровая гигиена?

а) Система защиты информации

б) Мера безопасности для защиты информации

в) Совокупность правил и рекомендаций, направленных на защиту информации, при использовании сети Интернет

4. Что такое конфиденциальность?

а) Сохранение целостности информации

б) Сохранение доступности информации

в) состояние, при котором информация доступна только для авторизованных пользователей, а все остальные не могут узнать ее содержание.

5. Что такое фишинг?

а) вирус, который заражает компьютеры

б) метод социальной инженерии, используемый злоумышленниками для получения конфиденциальной информации

в) спам-рассылка, которая содержит вирусы

6. Что такое фишинговые сайты?

а) сайты, которые содержат вирусы

б) сайты, которые используются для мошенничества и получения личной информации

в) сайты, которые содержат важную информацию для получения выгоды

7. Что такое фишинговые телефонные звонки?

а) звонки, которые используются для маркетинга

б) мошенничество, которое использует телефонные звонки для получения личной информации или выгоды

в) мошенничество, которое использует телефон жертвы

8. Что такое социальный фишинг?

а) мошенничество, которое использует социальные сети для получения личной информации

б) маркетинговый метод, который используется для продвижения товаров в социальных сетях

в) сообщения, которые отправляются с целью продвижения товаров в социальных сетях

9. Что такое SSL-сертификат?

а) вирус, который защищает компьютеры

б) сертификат, который используется для защиты личной информации

в) сертификат, который используется для продвижения товаров

10. Что такое аккаунт?

а) Это специальный компьютерный вирус, который может заразить вашу систему.

б) Это имя и пароль для доступа к определенному веб-сайту, сервису или приложению.

в) Это общее название для всех интернет-сервисов.

11. Что такое HTTPS?

а) Это технология, которая позволяет защищать вашу локальную сеть.

б) Это протокол, который обеспечивает безопасную передачу данных между веб-сайтом и пользователем.

в) Это название для специального вируса, который может заразить ваш компьютер.

12. Что такое банковские данные?

а) Это информация о том, какие продукты вы покупаете в интернет-магазинах.

б) Это информация о ваших личных финансах, включая номера банковских карт и счетов.

в) Это информация о ваших друзьях и знакомых.

13. Что такое двухфакторная авторизация?

а) Это система, которая позволяет защитить вашу систему от вирусов.

б) Это метод защиты, который требует ввода двух паролей для получения доступа к информации.

в) Это метод защиты, который требует ввода имени пользователя и пароля для получения доступа к информации.

14. Что такое оплата онлайн?

а) Это процесс покупки товаров в магазине, где вы должны заплатить наличными деньгами.

б) Это процесс покупки товаров в сети, где вы должны заплатить с помощью данных кредитной карты.

в) Это процесс покупки товаров в сети, где вы должны заплатить с помощью наличных денег.

15. Что такое безопасность в сети Интернет?

а) Защита от компьютерных вирусов

б) Защита личной информации и предотвращение кибератак

в) Ограничение доступа к определенным сайтам

16. Какие данные являются персональной информацией?

а) Имя, фамилия, адрес электронной почты

б) Номер телефона, дата рождения, место работы

в) Все вышеперечисленное

17. Что такое цифровая гигиена?

а) Соблюдение правил поведения в социальных сетях

б) Соблюдение правил поведения в сети Интернет

в) Соблюдение правил пользования мессенджерами

18. Какую информацию можно распространять публично?

а) Имя и фамилию

б) Адрес проживания

в) Никакую из вышеперечисленного

19. К какой категории данных относятся пароли для доступа к аккаунту или устройству?

а) Персональная информация

б) Конфиденциальная информация

в) Публичная (открытая) информация

20. Какое из перечисленных действий является примером безопасного поведения в сети Интернет?

а) Использование одного и того же пароля для разных аккаунтов

б) Сохранение паролей на бумажке, которую можно найти рядом с компьютером

в) Регулярное обновление программ и антивирусов

**3.2 Тест Вариант № 2»**

1. Что такое социальная инженерия?

а) технический метод защиты информации

б) техника взлома с помощью манипуляций

в) защита от вирусов

2. Что такое фишинг?

а) вирус, который заражает компьютеры

б) метод социальной инженерии, используемый злоумышленниками для получения конфиденциальной информации

в) спам-рассылка, которая содержит вирусы

3. Что такое фишинговые сайты?

а) сайты, которые содержат вирусы

б) сайты, которые используются для мошенничества и получения личной информации

в) сайты, которые содержат важную информацию для получения выгоды

4. Что такое приватная информация?

а) Информация, которая доступна только для определенных лиц

б) Информация, которая должна быть защищена

в) Информация, которая может быть свободно доступна всем

5. Что такое цифровая гигиена?

а) Система защиты информации

б) Мера безопасности для защиты информации

в) Совокупность правил и рекомендаций, направленных на защиту информации, при использовании сети Интернет

6. Что такое конфиденциальность?

а) Сохранение целостности информации

б) Сохранение доступности информации

в) состояние, при котором информация доступна только для авторизованных пользователей, а все остальные не могут узнать ее содержание.

7. Что такое фишинговые телефонные звонки?

а) звонки, которые используются для маркетинга

б) мошенничество, которое использует телефонные звонки для получения личной информации или выгоды

в) мошенничество, которое использует телефон жертвы

8. Что такое социальный фишинг?

а) мошенничество, которое использует социальные сети для получения личной информации

б) маркетинговый метод, который используется для продвижения товаров в социальных сетях

в) сообщения, которые отправляются с целью продвижения товаров в социальных сетях

9. Что такое SSL-сертификат?

а) вирус, который защищает компьютеры

б) сертификат, который используется для защиты личной информации

в) сертификат, который используется для продвижения товаров

10. Что такое аккаунт?

а) Это специальный компьютерный вирус, который может заразить вашу систему.

б) Это имя и пароль для доступа к определенному веб-сайту, сервису или приложению.

в) Это общее название для всех интернет-сервисов.

11. Что такое HTTPS?

а) Это технология, которая позволяет защищать вашу локальную сеть.

б) Это протокол, который обеспечивает безопасную передачу данных между веб-сайтом и пользователем.

в) Это название для специального вируса, который может заразить ваш компьютер.

12. Что такое банковские данные?

а) Это информация о том, какие продукты вы покупаете в интернет-магазинах.

б) Это информация о ваших личных финансах, включая номера банковских карт и счетов.

в) Это информация о ваших друзьях и знакомых.

13. Что такое двухфакторная авторизация?

а) Это система, которая позволяет защитить вашу систему от вирусов.

б) Это метод защиты, который требует ввода двух паролей для получения доступа к информации.

в) Это метод защиты, который требует ввода имени пользователя и пароля для получения доступа к информации.

14. Что такое оплата онлайн?

а) Это процесс покупки товаров в магазине, где вы должны заплатить наличными деньгами.

б) Это процесс покупки товаров в сети, где вы должны заплатить с помощью данных кредитной карты.

в) Это процесс покупки товаров в сети, где вы должны заплатить с помощью наличных денег.

15. Что такое безопасность в сети Интернет?

а) Защита от компьютерных вирусов

б) Защита личной информации и предотвращение кибератак

в) Ограничение доступа к определенным сайтам

16. Какие данные являются персональной информацией?

а) Имя, фамилия, адрес электронной почты

б) Номер телефона, дата рождения, место работы

в) Все вышеперечисленное

17. Что такое цифровая гигиена?

а) Соблюдение правил поведения в социальных сетях

б) Соблюдение правил поведения в сети Интернет

в) Соблюдение правил пользования мессенджерами

18. К какой категории данных относятся пароли для доступа к аккаунту или устройству?

а) Персональная информация

б) Конфиденциальная информация

в) Публичная (открытая) информация

19. Какое из перечисленных действий является примером безопасного поведения в сети Интернет?

а) Использование одного и того же пароля для разных аккаунтов

б) Сохранение паролей на бумажке, которую можно найти рядом с компьютером

в) Регулярное обновление программ и антивирусов

20. Какую информацию можно распространять публично?

а) Имя и фамилию

б) Адрес проживания

в) Никакую из вышеперечисленного

**3.3 Тест Вариант № 3»**

1. Какую информацию не следует размещать в социальных сетях?

а) контактную информацию

б) фотографии домашнего питомца

в) рецепты блюд

2. Что такое SSL-сертификат?

а) вирус, который защищает компьютеры

б) сертификат, который используется для защиты личной информации

в) сертификат, который используется для продвижения товаров

3. Что такое аккаунт?

а) Это специальный компьютерный вирус, который может заразить вашу систему.

б) Это имя и пароль для доступа к определенному веб-сайту, сервису или приложению.

в) Это общее название для всех интернет-сервисов.

4. Что такое HTTPS?

а) Это технология, которая позволяет защищать вашу локальную сеть.

б) Это протокол, который обеспечивает безопасную передачу данных между веб-сайтом и пользователем.

в) Это название для специального вируса, который может заразить ваш компьютер.

5. Что такое приватная информация?

а) Информация, которая доступна только для определенных лиц

б) Информация, которая должна быть защищена

в) Информация, которая может быть свободно доступна всем

6. Что такое цифровая гигиена?

а) Система защиты информации

б) Мера безопасности для защиты информации

в) Совокупность правил и рекомендаций, направленных на защиту информации, при использовании сети Интернет

7. Что такое конфиденциальность?

а) Сохранение целостности информации

б) Сохранение доступности информации

в) состояние, при котором информация доступна только для авторизованных пользователей, а все остальные не могут узнать ее содержание.

8. Что такое фишинг?

а) вирус, который заражает компьютеры

б) метод социальной инженерии, используемый злоумышленниками для получения конфиденциальной информации

в) спам-рассылка, которая содержит вирусы

9. Что такое фишинговые сайты?

а) сайты, которые содержат вирусы

б) сайты, которые используются для мошенничества и получения личной информации

в) сайты, которые содержат важную информацию для получения выгоды

10. Что такое фишинговые телефонные звонки?

а) звонки, которые используются для маркетинга

б) мошенничество, которое использует телефонные звонки для получения личной информации или выгоды

в) мошенничество, которое использует телефон жертвы

11. Что такое социальный фишинг?

а) мошенничество, которое использует социальные сети для получения личной информации

б) маркетинговый метод, который используется для продвижения товаров в социальных сетях

в) сообщения, которые отправляются с целью продвижения товаров в социальных сетях

12. Что такое банковские данные?

а) Это информация о том, какие продукты вы покупаете в интернет-магазинах.

б) Это информация о ваших личных финансах, включая номера банковских карт и счетов.

в) Это информация о ваших друзьях и знакомых.

13. Что такое двухфакторная авторизация?

а) Это система, которая позволяет защитить вашу систему от вирусов.

б) Это метод защиты, который требует ввода двух паролей для получения доступа к информации.

в) Это метод защиты, который требует ввода имени пользователя и пароля для получения доступа к информации.

14. Что такое оплата онлайн?

а) Это процесс покупки товаров в магазине, где вы должны заплатить наличными деньгами.

б) Это процесс покупки товаров в сети, где вы должны заплатить с помощью данных кредитной карты.

в) Это процесс покупки товаров в сети, где вы должны заплатить с помощью наличных денег.

15. Что такое безопасность в сети Интернет?

а) Защита от компьютерных вирусов

б) Защита личной информации и предотвращение кибератак

в) Ограничение доступа к определенным сайтам

16. Какие данные являются персональной информацией?

а) Имя, фамилия, адрес электронной почты

б) Номер телефона, дата рождения, место работы

в) Все вышеперечисленное

17. Что такое цифровая гигиена?

а) Соблюдение правил поведения в социальных сетях

б) Соблюдение правил поведения в сети Интернет

в) Соблюдение правил пользования мессенджерами

18. Какую информацию можно распространять публично?

а) Имя и фамилию

б) Адрес проживания

в) Никакую из вышеперечисленного

19. К какой категории данных относятся пароли для доступа к аккаунту или устройству?

а) Персональная информация

б) Конфиденциальная информация

в) Публичная (открытая) информация

20. Какое из перечисленных действий является примером безопасного поведения в сети Интернет?

а) Использование одного и того же пароля для разных аккаунтов

б) Сохранение паролей на бумажке, которую можно найти рядом с компьютером

в) Регулярное обновление программ и антивирусов

Ответ: в)

**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 |