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» (10-11 классов)

**СБОРНИК**

**Контрольно-измерительных материалов**

**(КИМы)**

**(2-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» 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 за все время обучения 10-11 классов:

|  |  |
| --- | --- |
| 1 | Введение в информационную безопасность |
| 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. |
| 1.5 | Основные нормативные руководящие документы информационной безопасности. |
| 1.6 | Понятие государственной тайны. Виды секретности. |
| 1.7 | Международные стандарты в сфере информационной безопасности. |
| 1.8 | Уголовный и административный кодекс правонарушений. Ответственность в сфере информационной безопасности. |
| 1.9 | Публикация персональной информации. Приватность и конфиденциальность в сети. |
| 1.10 | Фишинг. Варианты воздействия и способы защиты. |
| 1.11 | Социальная инженерия. Правила безопасности при общении в сети. |
| 1.12 | Безопасность аккаунтов в сети. Совершение покупок онлайн. |
| 1.13 | Система как объект информационных воздействий и управления. |
| 1.14 | Концепция сетецентрической и информационной войны. |
| 1.15 | Информационное противоборство в психологической сфере. |
| 1.16 | Когнитивная самооборона в условиях информационного противоборства. |

*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 | 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 |
| 1.5 | Основные нормативные руководящие документы информационной безопасности. | Законы и руководящие документы РФ в сфере информационной безопасности. Доктрина информационной безопасности. Ведомства и их роль в обеспечении информационной безопасности государства. Понятие критически важных объектов информационной инфраструктуры. | Не предусмотрен |  |  |  |  |
| 1.6 | Понятие государственной тайны. Виды секретности. | Понятие грифа секретности. Ограничения и ответственность, накладываемые на носителя государственной тайны. Процедура допуска к государственной тайне. | Не предусмотрен |
| 1.7 | Международные стандарты в сфере информационной безопасности. | Руководящие документы и стандарты, принятые международным сообществом в информационной сфере. Рекомендации по обеспечению информационной безопасности. Методы оценки рисков безопасности информационной системы. | Не предусмотрен |
| 1.8 | Уголовный и административный кодекс правонарушений. Ответственность в сфере информационной безопасности. | Изучение уголовного и административного кодекса правонарушений с целью ознакомления со статьями, связанными с информационной безопасностью. Понятие правонарушение и наказания. Разбор на конкретных примерах правомерности действий при работе с информацией. | Не предусмотрен |
| 1.9 | 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 |
| 1.10 | Фишинг. Варианты воздействия и способы защиты. | Понятие фишинга. Механизм работы фишинга. Примеры применения и способы защиты. | Не предусмотрен |
| 1.11 | 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 |
| 1.12 | 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 |
| 1.13 | Система как объект информационных воздействий и управления. | Понятие информационного воздействия. Системный подход к проблеме информационного воздействия. Виды управления с помощью воздействия на информационную сферу. | Не предусмотрен |
| 1.14 | Концепция сетецентрической и информационной войны. | Понятие сетецентрической модели. Понятие информационной войны. Современные тенденции по повышению роли информационных средств при ведении противостояния. Основные особенности сетецентрической войны. Возможности ассиметричного противодействия в сетецентрической войне. | Не предусмотрен |
| 1.15 | Информационное противоборство в психологической сфере. | Основы информационно-психологического противоборства. Средства массовой информации. Средства на основе интернет-ресурсов и социальных сетей. Средства предъявления неосознаваемой информации. | Не предусмотрен |
| 1.16 | Когнитивная самооборона в условиях информационного противоборства. | Понятие когнитивного воздействия. Примеры когнитивного воздействия. Выработка модели поведения в целях минимизации когнитивного воздействия. | Не предусмотрен |

**3. Спецификация контрольных измерительных материалов**

**3.1 Тест Вариант № 1**

1. Что такое анализ рисков?

а) Оценка возможных угроз для информационной безопасности.

б) Процесс определения доступности информации для пользователя.

в) Способность системы информационной безопасности справляться с возможными атаками.

1. Что такое тестирование на проникновение?

а) Попытка несанкционированного доступа к системе для оценки ее уязвимостей.

б) Использование специальных программ для защиты компьютера от вирусов.

в) Оценка доступности информации для пользователя.

3. Что регулирует Федеральный закон “О защите детей от информации, причиняющей вред их здоровью и развитию”?

а) Защиту детей от информации, причиняющей вред их здоровью и развитию

б) Правила использования информационных технологий на территории России

в) Правила использования открытых сетей на территории России

4. Что такое персональные данные?

а) Информация, относящаяся к конкретному человеку, которую можно использовать для его идентификации

б) Информация, относящаяся к компании, которую можно использовать для ее идентификации

5. Что регулирует Федеральный закон "О связи"?

а) Правила использования средств связи на территории России

б) Правила использования информационных технологий на территории России

в) Условия доступа к государственной тайне на территории России

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. 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 сетецентрическая среда?

а) Среда, в которой используются только сетевые технологии

б) Среда, в которой сетевые технологии используются как основное средство передачи информации

в) Среда, в которой сетевые технологии не используются

18. Что такое сетецентрические операции?

а) Операции, в которых используются только сетевые технологии

б) Операции, в которых сетевые технологии используются как основное средство передачи информации

в) Операции, в которых сетевые технологии не используются

19) Что такое когнитивное воздействие?

а) Заражение компьютера вредоносным ПО

б) Воздействие на умственные процессы человека

в) Фишинговая атака на электронную почту

20) Что такое критическое мышление?

а) Анализ и оценка информации с целью принятия обоснованного решения

б) Подход к решению проблемы без использования логического мышления

в) Принятие решения на основе предубеждений

Ответ: a)

**3.2 Тест Вариант № 2**

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. Что регулирует Федеральный закон "О связи"?

а) Правила использования средств связи на территории России

б) Правила использования информационных технологий на территории России

в) Условия доступа к государственной тайне на территории России

6. Что такое государственная тайна?

а) Это информация, которую государство считает важной для своей безопасности и не желает раскрывать общественности.

б) Это информация, которая является главным секретом правительства.

в) Это информация, которая не имеет отношения к безопасности государства.

7. Какие бывают три степени секретности?

а) Секретно, очень секретно, государственная тайна.

б) Секретно, совершенно секретно, особой важности.

в) Секретно, строго секретно, очень строго секретно.

8. Что такое коммерческая тайна?

а) Это информация, которую компании считают важной для своего бизнеса и не желают раскрывать конкурентам и общественности.

б) Это информация, которая является главным секретом компании.

в) Это информация, которая не имеет отношения к бизнесу компании.

9. Что такое тайна личной жизни?

а) Это информация, которая не имеет отношения к личной жизни человека.

б) Это информация, которая относится к личной жизни человека и не должна быть раскрыта без его согласия.

в) Это информация, которая может быть раскрыта без согласия человека.

10. Что такое Международные стандарты в сфере информационной безопасности?

а) Документы, определяющие правила и требования к информационной безопасности на международном уровне.

б) Специальное программное обеспечение для защиты информации на компьютере.

в) Компьютерные игры, направленные на обучение правилам информационной безопасности.

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. Что такое система в контексте информационной безопасности?

а) Компьютерная программа

б) Комплекс взаимосвязанных элементов, которые работают вместе для достижения определенной цели

в) Способ зашифровки данных

17. Что такое управление?

а) Процесс обнаружения уязвимостей в системе

б) Процесс целенаправленного изменения состояния или выхода некоторой управляемой подсистемы

в) Способ защиты компьютерной сети от взлома

18. Что такое информационное воздействие?

а) Нарушение конфиденциальности информации

б) Попытка получения несанкционированного доступа к информации

в) Способ влияния на мнение людей через распространение определенной информации

19. Что такое психологическое воздействие в контексте информационной безопасности?

а) Процесс обучения пользователей правильному использованию компьютерной техники

б) Способ защиты информации от несанкционированного доступа

в) Использование психологических методов и технологий для воздействия на эмоции, мнения и поведение людей.

20. Что такое сетецентрическая война?

а) Война, в которой используются только сетевые технологии

б) Война, в которой сетевые технологии используются как основное оружие

в) Война, в которой сетевые технологии не используются

**3.3 Тест Вариант № 3**

1. Что такое Доктрина информационной безопасности России?

а) Совокупность официальных документов, определяющих основные направления государственной политики в области информационной безопасности России

б) Журнал, в котором публикуются новости и статьи о сфере информационной безопасности России

в) Книга, написанная российскими учеными, рассказывающая о проблемах информационной безопасности в России

2. Что регулирует Федеральный закон "О защите персональных данных"?

а) Правила использования персональных данных на территории России

б) Условия использования персональных данных на территории России

в) Правила использования открытых сетей на территории России

3. Что регулирует Федеральный закон “О защите детей от информации, причиняющей вред их здоровью и развитию”?

а) Защиту детей от информации, причиняющей вред их здоровью и развитию

б) Правила использования информационных технологий на территории России

в) Правила использования открытых сетей на территории России

4. Что такое персональные данные?

а) Информация, относящаяся к конкретному человеку, которую можно использовать для его идентификации

б) Информация, относящаяся к компании, которую можно использовать для ее идентификации

5. Что регулирует Федеральный закон "О связи"?

а) Правила использования средств связи на территории России

б) Правила использования информационных технологий на территории России

в) Условия доступа к государственной тайне на территории России

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. 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 сетецентрическая среда?

а) Среда, в которой используются только сетевые технологии

б) Среда, в которой сетевые технологии используются как основное средство передачи информации

в) Среда, в которой сетевые технологии не используются

18. Что такое сетецентрические операции?

а) Операции, в которых используются только сетевые технологии

б) Операции, в которых сетевые технологии используются как основное средство передачи информации

в) Операции, в которых сетевые технологии не используются

19. Что такое асимметричность информации?

а) Ситуация, когда информация передается от одного источника к другому без изменений

б) Ситуация, когда информация передается от одного источника к другому с изменениями

в) Ситуация, когда одна сторона обладает большим количеством информации, чем другая

20. Что такое психологическая война?

а) Борьба, в которой используются только психологические методы воздействия

б) Борьба между государствами и их вооруженными силами за достижение превосходства в психологической и духовной сферах

в) Война, в которой психологические методы используются только в защите

**3.2 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 – 1.16 | Б | 5 | 10 |