ПРИМЕР ОЦЕНОЧНОГО СРЕДСТВА

для оценки квалификации

**Специалист в области защиты информации на атомных станциях (6 уровень квалификации)**

(6 уровень квалификации)

Состав примера оценочных средств

|  |  |
| --- | --- |
| Раздел | Страница |
| 1. Наименование квалификации и уровень квалификации | 3 |
| 2. Номер квалификации | 3 |
| 3. Профессиональный стандарт или квалификационные требования, установленные федеральными законами и иными нормативными правовыми актами Российской Федерации | 3 |
| 4. Вид профессиональной деятельности | 3 |
| 5. Спецификация заданий для теоретического этапа профессионального экзамена | 3 |
| 6. Спецификация заданий для практического этапа профессионального экзамена | 4 |
| 7. Материально-техническое обеспечение оценочных мероприятий | 4 |
| 8. Кадровое обеспечение оценочных мероприятий | 4 |
| 9. Требования безопасности к проведению оценочных мероприятий | 5 |
| 10. Задания для теоретического этапа профессионального экзамена | 5 |
| 11. Критерии оценки (ключи к заданиям), правила обработки результатов теоретического этапа профессионального экзамена и принятия решения о допуске (отказе в допуске) к практическому этапу профессионального экзамена | 11 |
| 12. Задания для практического этапа профессионального экзамена | 12 |
| 13. Правила обработки результатов профессионального экзамена и принятия решения о соответствии квалификации соискателя требованиям к квалификации | 16 |
| 14. Перечень нормативных правовых и иных документов, использованных при подготовке комплекта оценочных средств | 16 |

1. Наименование квалификации и уровень квалификации: Специалист в области защиты информации на атомных станциях (6 уровень квалификации) (6 уровень квалификации).

2. Номер квалификации: 24.05700.02

3. Профессиональный стандарт или квалификационные требования, установленные федеральными законами и иными нормативными правовыми актами Российской Федерации (далее – требования к квалификации): 24.057 Специалист в области информационных технологий на атомных станциях (разработка и сопровождение программного обеспечения).

4. Вид профессиональной деятельности: Деятельность по обеспечению работоспособности атомных электростанций.

5. Спецификация заданий для теоретического этапа профессионального экзамена:

-

6. Спецификация заданий для практического этапа профессионального экзамена:

-

7. Материально-техническое обеспечение оценочных мероприятий:

а) материально-технические ресурсы для обеспечения теоретического этапа профессионального экзамена: аудитория, оборудованная персональным компьютером для соискателя, наличие интернет-соединения;

б) материально-технические ресурсы для обеспечения практического этапа профессионального экзамена: аудитория, оборудованная персональным компьютером для соискателя, наличие интернет-соединения.

8. Кадровое обеспечение оценочных мероприятий:

а) высшее образование (желательно наличие учёной степени);

б) опыт работы не менее 5 лет в сфере профессиональной деятельности, включающей оцениваемую квалификацию, не ниже уровня оцениваемой квалификации;

в) подтверждение квалификации эксперта со стороны Совета по профессиональным квалификациям в сфере атомной энергии.

9. Требования безопасности к проведению оценочных мероприятий (при необходимости): проведение инструктажа на рабочем месте пользователя компьютерной и оргтехникой, проведение инструктажа по пожарной и электробезопасности, оформление записей в соответствующих журналах.

10. Задания для теоретического этапа профессионального экзамена:

Задания с закрытым ответом

1. ***Укажите верное определение понятию «информационная безопасность».***

А) Состояние защищенности информации, обрабатываемой в автоматизированной системе, от внешних и внутренних угроз.

Б) Обеспечение защищенности информации, обрабатываемой в автоматизированной системе, от внешних и внутренних угроз.

В) Обеспечение защищенности жизненно важных интересов личности, общества и государства в информационной сфере.

Г) Состояние защищенности жизненно важных интересов личности, общества и государства от внешних и внутренних информационных угроз.

1. ***Укажите, в чем заключается фаза проявления компьютерного вируса.***

А) В заражении других программ.

Б) В разрушении программ и данных, предусмотренном автором вируса.

В) В многократном самокопировании вируса.

Г) В обнаружении антивирусным программным обеспечением.

1. ***Представьте следующую ситуацию: сотрудники атомной станции имеют одинаковую форму допуска и пытаются с помощью автоматизированной системы получить строго конфиденциальную информацию по вопросу расследования инцидентов. Какой из основных принципов защиты информации от несанкционированного доступа должен быть положен в основу принятия решения в данной ситуации?***

А) Принцип обоснованности доступа.

Б) Принцип достаточной глубины контроля доступа.

В) Принцип разграничения потоков информации.

Г) Принцип персональной ответственности.

1. ***Укажите, к какому из макропроцессов управления системой защиты информации относится принятие решения о корректировке антивирусного программного обеспечения.***

А) Планирование.

Б) Оперативно-диспетчерское управление.

В) Календарно-плановое руководство.

Г) Обеспечение повседневной деятельности системы управления.

1. ***Укажите, какое из перечисленных мероприятий необходимо для реализации контроля защищенности информации.***

А) Календарно-плановый контроль.

Б) Планирование контроля механизмов защиты.

В) Прогнозирование показателей защищенности информации.

Г) Накопление данных о параметрах защищенности информации.

1. ***Укажите, к какому из классов атак относится поддельное письмо, отправленное жертве по электронной почте, которое выглядит как официальное.***

А) Претекстинг.

Б) Кви-про-кво.

В) Фишинг.

Г) Атака полного перебора ключей.

1. ***Укажите верное определение понятию «троянский конь».***

А) Программа, которая тиражируется в памяти компьютера и распространяется по сети.

Б) Программа, которая находится внутри другой, как правило, абсолютно безобидной программы, при запуске которой в систему инсталлируется программа, написанная с целью нанесения ущерба целевому компьютеру путем выполнения несанкционированных пользователем действий.

В) Программа, установленная на компьютер без согласия его владельца

Г) Программа, которая несанкционированного зашифровывает данные в памяти компьютера.

1. ***Укажите термин, соответствующий определению: «получение доступа к данным, хранящимся на различных носителях и накопителях, посредством самовольного изменения или же фальсификации соответствующих прав».***

А) Идентификация.

Б) Аутентификация.

В) Авторизация.

Г) Несанкционированный доступ.

1. ***Укажите, какие персональные данные не являются специальными.***

А) Данные о состоянии здоровья.

Б) Данные о расовой принадлежности.

В) Отпечатки пальцев.

Г) Данные о философских убеждениях.

1. ***Укажите, какие из приведенных данных не содержатся в сертификате ключа проверки электронной подписи для физического лица.***

А) Фамилия, имя, отчество.

Б) Семейное положение.

В) Дата начала и окончания срока действия сертификата.

Г) Ключ проверки электронной подписи.

1. ***Укажите, какую функцию не может выполнять SIEM-решение.***

А) Отслеживание атак на веб-приложения.

Б) Обнаружение кражи данных.

В) Мониторинг подозрительного исходящего трафика.

Г) Реагирование на инцидент.

1. ***Укажите, для чего может быть использована криптографическая система ГОСТ 28147-89?***

А) Для шифрования.

Б) Для выработки электронной подписи.

В) Для выработки общего ключа между пользователями.

Г) Для защиты от вирусов.

1. ***Укажите компонент инфраструктуры открытых ключей.***

А) Центр сертификации.

Б) Криптографический примитив.

В) Криптографический протокол.

Г) Политика сертификации.

Задания на указание последовательности

1. ***Расположите правильно в виде последовательности цифр приведённые ниже действия, предусмотренные типовым алгоритмом, реализуемым программой-вирусом.***
2. Проверить условие срабатывания.
3. При выполнении условия осуществить заданные манипуляции, при невыполнении – передать управление несущей вирус программе.
4. Найти и заразить незараженную программу.
5. ***Расположите правильно в виде последовательности цифр приведённые ниже действия при реализации комплексной стратегии предотвращения вирусного подавления.***
6. Обнаружение.
7. Альтернативные меры.
8. Ликвидация.
9. Сдерживание.
10. Восстановление нормального функционирования.
11. ***Расположите правильно в виде последовательности цифр приведённые ниже действия при решении задач выработки требований по защите информации.***
12. Структурированное описание требований к защите в пределах выделенных классов.
13. Формирование перечня и классификация факторов, влияющих на требуемый уровень защиты.
14. Структуризация возможных значений факторов.
15. Оптимальное деление поля возможных вариантов на типовые классы.
16. Структуризация поля потенциально возможных вариантов условий защиты.
17. Разработка методов оценки параметров защищаемой информации.
18. ***Расположите правильно в виде последовательности цифр приведённые ниже действия при реализации оперативно-диспетчерского управления защитой информации в аварийной ситуации.***
19. Доложить руководству и информировать пользователей.
20. Проверить достоверность сведений, на основании которых ситуация отнесена к аварийной.
21. Принять неотложные меры.
22. ***Расположите правильно в виде последовательности цифр приведённые ниже действия, предусмотренные схемой электронной подписи вслепую.***
23. Выработка параметров.
24. Выработка подписи к сообщению.
25. Затемнение сообщения.
26. Проверка подписи.
27. Выделение подписи к оригинальному сообщению.
28. ***Расположите правильно в виде последовательности цифр приведённые ниже нормативные правовые документы в области информационной безопасности в порядке убывания значимости.***
29. Законы федерального уровня.
30. Указы Президента РФ.
31. Нормативные правовые акты субъектов РФ.
32. Конституция РФ.
33. Постановления Правительства РФ.
34. Приказы ФСТЭК России, ФСБ России.
35. ***Расположите правильно в виде последовательности цифр приведённые ниже действия при проверке работоспособности системы обнаружения вторжений.***
36. Смоделировать атаку.
37. Написать правила на детектирование атаки.
38. Установить систему.
39. Проверить журнал на наличие реакции.

Задания на установление соответствия

1. ***Установите соответствие принципа информационной безопасности его названию. Для этого каждой позиции левой части таблицы (А, Б, В) найдите соответствие в правой части таблицы (1, 2, 3, 4, 5, 6). Для ответа впишите цифру от 1 до 6, соответствующую, по Вашему мнению, верному ответу, на месте многоточия. А – … Б – … В – …***

|  |  |
| --- | --- |
| А) Принцип персональной ответственности | 1) Пользователь должен иметь необходимую форму допуска, соответствующую уровню конфиденциальности запрашиваемой информации |
| Б) Принцип достаточной глубины контроля доступа | 2) Пользователь должен быть аутентифицирован |
| В) Принцип обоснованности доступа | 3) Информация разного уровня конфиденциальности передавалась в разных потоках |
|  | 4) Система защиты информации должна быть изолированной от пользователей |
|  | 5) Должна быть предусмотрена очистка ресурсов, содержащих конфиденциальную информацию, до их перераспределения другим пользователя |
|  | 6) Механизмы контроля должны охватывать все информационные массивы, которые разграничиваются между пользователями |

1. ***Установите соответствие между задачами обеспечения информационной безопасности и подходами к их решению. Для этого каждой позиции левой части таблицы (А, Б, В) найдите соответствие в правой части таблицы (1, 2, 3, 4). Для ответа впишите цифру от 1 до 4, соответствующую, по Вашему мнению, верному ответу, на месте многоточия. А – … Б – … В – …***

|  |  |
| --- | --- |
| А) Концептуально-эмпирический подход | 1) Комплексное обеспечение компьютерной безопасности |
| Б) Теоретико-концептуальный подход | 2) Комплексное обеспечение безопасности объекта |
| В) Общетеоретический подход | 3) Обеспечение информационной безопасности государства |
|  | 4) Антивирусная защита |

1. ***Установите соответствие между методами защиты информации и средствами, которые их реализуют. Для этого каждой позиции левой части таблицы (А, Б, В) найдите соответствие в правой части таблицы (1, 2, 3, 4). Для ответа впишите цифру от 1 до 4, соответствующую, по Вашему мнению, верному ответу, на месте многоточия. А – … Б – … В – …***

|  |  |
| --- | --- |
| А) Криптографические средства | 1) Шифрование информации |
| Б) Технические средства | 2) Разграничение доступа к информации |
| В) Организационно-правовые средства | 3) Регулирование прав и обязанностей при обработке информации |
|  | 4) Обнаружение вирусов |

1. ***Установите соответствие номера статьи Уголовного кодекса РФ ее названию. Для этого каждой позиции левой части таблицы (А, Б, В) найдите соответствие в правой части таблицы (1, 2, 3, 4). Для ответа впишите цифру от 1 до 4, соответствующую, по Вашему мнению, верному ответу, на месте многоточия. А – … Б – … В – …***

|  |  |
| --- | --- |
| А) 272 | 1) Государственная измена |
| Б) 273 | 2) Создание, использование и распространение вредоносных программ для ЭВМ |
| В) 275 | 3) Неправомерный доступ к компьютерной информации |
|  | 4) Нарушение тайны переписки, телефонных переговоров, почтовых, телеграфных или иных сообщений |

1. ***Установите соответствие номера Федерального закона РФ его названию. Для этого каждой позиции левой части таблицы (А, Б, В) найдите соответствие в правой части таблицы (1, 2, 3, 4, 5). Для ответа впишите цифру от 1 до 5, соответствующую, по Вашему мнению, верному ответу, на месте многоточия. А – … Б – … В – …***

|  |  |
| --- | --- |
| А) 149-ФЗ | 1) Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных |
| Б) 152-ФЗ | 2) О персональных данных |
| В) 187-ФЗ | 3) Об информации, информационных технологиях и защите информации |
|  | 4) О безопасности критической информационной инфраструктуры Российской Федерации |
|  | 5) Об электронной подписи |

1. ***Установите соответствие типа программно-аппаратного средства защиты информации его названию. Для этого каждой позиции левой части таблицы (А, Б, В) найдите соответствие в правой части таблицы (1, 2, 3, 4). Для ответа впишите цифру от 1 до 4, соответствующую, по Вашему мнению, верному ответу, на месте многоточия. А – … Б – … В – …***

|  |  |
| --- | --- |
| А) Соболь | 1) Средство антивирусной защиты |
| Б) Notary PRO | 2) Средство обнаружения вторжений |
| В) Eset | 3) Средство защиты информации от несанкционированного доступа |
|  | 4) Средство криптографической защиты информации |

Задания с открытым ответом

1. ***Сколько уровней в эталонной модели взаимодействия открытых систем?***
2. ***Сколько уровней в модели взаимодействия систем TCP/IP?***
3. ***В каком году принят Федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации»?***
4. ***В каком году принят Федеральный закон «Об информации, информационных технологиях и защите информации»?***
5. ***В каком году принят Федеральный закон «Об электронной подписи»?***
6. ***В каком году принят Федеральный закон «О персональных данных»?***
7. ***Сколько существует категорий персональных данных?***
8. ***Сколько существует типов угроз безопасности персональным данным?***
9. ***Сколько существует уровней защищенности персональных данных?***
10. ***Укажите номер приказа ФСТЭК России, утверждающего требования к защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах?***
11. ***В каком году утверждена Доктрина информационной безопасности РФ?***
12. ***Сколько существует классов защищенности автоматизированных систем?***
13. ***Сколько существует классов защиты систем обнаружения вторжений?***
14. ***Укажите аббревиатуру (без указания «РФ» или «России») – сокращенное название организации, сертифицирующей средства криптографической защиты информации?***

11. Критерии оценки (ключи к заданиям), правила обработки результатов теоретического этапа профессионального экзамена и принятия решения о допуске (отказе в допуске) к практическому этапу профессионального экзамена:

**-**

12. Задания для практического этапа профессионального экзамена:

а) задание на выполнение трудовых функций, трудовых действий в реальных или модельных условиях:

- трудовая функция: **Обеспечение сохранности информации, защита информации от несанкционированного доступа**

- трудовое действие (действия): **Разработка предложений и рекомендаций по внедрению комплексных систем защиты информации**

Задание:

**Представить перечень действий, которые необходимо проводить в рамках внедрения организационных и технических мер по обеспечению безопасности значимого объекта критической информационной инфраструктуры Российской Федерации. Указать нормативный правовой акт, определяющий данный перечень.**

Условия выполнения задания:

**аудитория, оборудованная персональным компьютером для соискателя, наличие интернет-соединения**; **максимальное время выполнения задания – 30 минут.**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ЗАДАНИЕ НА ВЫПОЛНЕНИЕ ТРУДОВЫХ ФУНКЦИЙ, ТРУДОВЫХ ДЕЙСТВИЙ В РЕАЛЬНЫХ ИЛИ МОДЕЛЬНЫХ УСЛОВИЯХ  Типовое задание:  **Представить перечень действий, которые необходимо проводить в рамках внедрения организационных и технических мер по обеспечению безопасности значимого объекта критической информационной инфраструктуры Российской Федерации. Указать нормативный правовой акт, определяющий данный перечень.**   |  |  | | --- | --- | | **Трудовые функции, трудовые действия, умения в соответствии с требованиями к квалификации, на соответствие которым проводится оценка квалификации** | **Критерии оценки** | | Разработка предложений и рекомендаций по внедрению комплексных систем защиты информации | Задание выполнено полностью – 1 балл | | |
| Условия выполнения задания:  1. Место (время) выполнения задания: аудитория.  2. Максимальное время выполнения задания: 30 минут.  3. Вы можете воспользоваться:  - компьютер с интернет-соединением;  - ручка, бумага. |

б) задание на выполнение трудовых функций, трудовых действий в реальных или модельных условиях:

- трудовая функция: **Обеспечение сохранности информации, защита информации от несанкционированного доступа**

- трудовое действие (действия): **Организация системы разграничения доступа**

Задание:

**Представить состав мер по управлению доступом, принимаемых для обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, для трех категорий значимости. Указать нормативный правовой акт, определяющий данный состав.**

Условия выполнения задания:

**аудитория, оборудованная персональным компьютером для соискателя, наличие интернет-соединения; максимальное время выполнения задания – 30 минут**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| ЗАДАНИЕ НА ВЫПОЛНЕНИЕ ТРУДОВЫХ ФУНКЦИЙ, ТРУДОВЫХ ДЕЙСТВИЙ В РЕАЛЬНЫХ ИЛИ МОДЕЛЬНЫХ УСЛОВИЯХ  Типовое задание:  **Представить состав мер по управлению доступом, принимаемых для обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, для трех категорий значимости. Указать нормативный правовой акт, определяющий данный перечень.**   |  |  | | --- | --- | | **Трудовые функции, трудовые действия, умения в соответствии с требованиями к квалификации, на соответствие которым проводится оценка квалификации** | **Критерии оценки** | | Организация системы разграничения доступа | Задание выполнено полностью – 1 балл | | |
| Условия выполнения задания:  1. Место (время) выполнения задания: аудитория.  2. Максимальное время выполнения задания: 30 минут.  3. Вы можете воспользоваться:  - компьютер с интернет-соединением;  - ручка, бумага. |

Критерий принятия положительного решения относительно прохождения практической части экзамена соответствует 100 % выполненных заданий (2 балла).

в) задание для оформления и защиты портфолио: портфолио не предусмотрено

13. Правила обработки результатов профессионального экзамена и принятия решения о соответствии квалификации соискателя требованиям к квалификации: положительное решение о соответствии квалификации соискателя требованиям к квалификации по квалификации Специалист в области защиты информации на атомных станциях (6 уровень квалификации) принимается при совместном выполнении двух условий:

а) теоретическое задание должно быть выполнено не менее чем на 60 % (для допуска к практической части экзамена);

б) практические задания – задание 1 и задание 2 – должны быть выполнены с результатом 100%.

14. Перечень нормативных правовых и иных документов, использованных при подготовке комплекта оценочных средств:

1. Приказ ФСТЭК России от 25 декабря 2017 г. N 239.