**Областное государственное бюджетное профессиональное**

**образовательное учреждение**

**«Смоленская академия профессионального образования»**

«Утверждаю»

Заместитель директора по НМР

Н.В. Судденкова

 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

 « \_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_\_2014 г.

**Комплект контрольно-измерительных материалов по учебной дисциплине**

**ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

основной профессиональной образовательной программы (ОПОП)

по специальности СПО

**10.02.01 Организация и технология защиты информации**

**(базовая подготовка)**

2014 г.

Комплект контрольно-измерительных материалов по учебной дисциплине Информационная безопасность разработан на основе Федерального государственного образовательного стандарта по специальности СПО 10.02.01 Организация и технология защиты информации (базовая подготовка)

Организация разработчик: ОГБПОУ «Смоленская академия профессионального образования»

Разработчик: Ромашкова И.И., преподаватель специальных дисциплин кафедры Информационных технологий

Рассмотрено на заседании кафедры Информационных технологий

Протокол №\_\_\_\_ от «\_\_\_\_»\_\_\_\_\_\_\_2014г.

Зав. кафедрой (декан)\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Малахова В.Г.

Рассмотрено научно-методическим советом ОГБПОУ «Смоленская академия профессионального образования»

Протокол №\_\_\_ от «\_\_\_»\_\_\_\_\_2014г.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Содержание

1. Паспорт комплекта контрольно-оценочных средств..........................................................................4

1.1. Область применения.......................................................................................................................4

* 1. Система контроля и оценки освоения программы учебной дисциплины .................................4
		1. Форма итоговой аттестации по ОПОП при освоении учебной дисциплины.................4

1.2.2. Организация контроля и оценки освоения программы ОП..................................................4

2. Комплект материалов для оценки освоенных умений и усвоенных знаний по дисциплине «Основы информационной безопасности»......................................................................................................6

3. Пакет экзаменатора................................................................................................................................10

4. Приложение Вопросы теста ………………………………………………………………………….11

**I. Паспорт комплекта контрольно-оценочных средств**

**1.1. Область применения**

Комплект контрольно-измерительных материалов предназначен для проверки результатов освоения общепрофессиональной дисциплины *Основы информационной безопасности* по специальности 10.02.01 Организация и технология защиты информации.

**Комплект контрольно-оценочных средств позволяет оценивать:**

* + 1. Освоение умений и усвоение знаний:

|  |  |  |
| --- | --- | --- |
| **Знания и умения для проверки** | **Показатели оценки результата** | **№ заданий****для проверки** |
| Классифицировать защищаемую информацию по видам тайны и степеням конфиденциальности | - Правильность соотнесения защищаемой информации видам тайн и степеням конфиденциальности в соответствии с классификацией | Практическое задание |
| Применять правовые правила и документы системы сертификации Российской Федерации | - Правильность применения правовых правил и документов системы сертификации РФ |
| Классифицировать основные угрозы безопасности информации | - Правильность определения угроз безопасности информации в соответствии с классификацией |
| Знать сущность и понятия информационной безопасности, характеристику ее составляющих; | - Правильность изложения сущности ИБ- Правильность соотнесения понятий информационной безопасности с их определениями. | Вопросы теста |
| Знать место информационной безопасности в системе национальной безопасности страны | - Правильность схематичного представления системы национальной безопасности страны.- Правильность определения места информационной безопасности в системе национальной безопасности страны. | Вопросы теста |
| Знать источники угроз информационной безопасности и мер по их предотвращению | - Правильность определения источников угроз информационной безопасности для заданного объекта- Соответствие выбранных мер вероятности их реализации угроз | Вопросы теста |
| Знать жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи;  | - Правильность построения логической последовательности жизненного цикла конфиденциальной информации | Вопросы теста |
| Знать современные средства и способы обеспечения информационной безопасности; | - Точность изложения способов обеспечения информационной безопасности.- Соответствие выбранных средств обеспечения ИБ степени конфиденциальности информации. | Вопросы теста |

**1.2 Система контроля и оценки освоения программы учебной дисциплины**

Текущий контроль освоения программы дисциплины предусматривает рейтинговую систему оценки и проводится в пределах учебного времени, отведенного на её изучение, с использованием таких методов, как написание самостоятельных работ, контрольных работ, выполнение тестов, проведение устного опроса, выполнение практических работ.

Оценка освоения программы дисциплины проводится в соответствии с «Положением о промежуточной аттестации» и рабочим учебным планом в форме экзамена.

* + 1. **Форма итоговой аттестации по ОПОП при освоении учебной дисциплины:**

Экзамен проводится в виде компьютерного тестирования в программе «СПО-ТЕСТ» (теоретическая часть) и устного собеседования по билетам.

**1.2.2. Организация контроля и оценки освоения программы ОП**

Итоговый контроль освоения дисциплины «Основы информационной безопасности» осуществляется на экзамене. Условием допуска к экзамену является положительная текущая аттестация по всем практическим работам учебной дисциплины, ключевым теоретическим вопросам дисциплины (проверка выполняется текущим контролем).

**2. Комплект материалов для оценки освоенных умений и усвоенных знаний по дисциплине** *Основы информационной безопасности*

ЗАДАНИЯ ДЛЯ ЭКЗАМЕНУЮЩИХСЯ № 1

**Условия выполнения задания:**

Задание выполняется в учебной аудитории.

Используемое оборудование: компьютеры с установленным необходимым программным обеспечением, оборудование для программно-технической защиты информации.

**Инструкция:**

1.Задание выполняется в два этапа:

- дайте ответы на предложенные Вам теоретические вопросы в программе «СПО-ТЕСТ»;

- решите предложенную задачу.

2. При выполнении решения задачи вы можете воспользоваться компьютером, калькулятором, необходимым оборудованием по программно-технической защите информации.

3. Максимальное время выполнения задания – 60 мин. (теоретическое задание – 30 мин., задача – 30 мин.)

**Образец экзаменационного билета**

**Вариант 1**

|  |
| --- |
| 1. Тест.2. Осуществите проверку правильности классификации угроз информационной безопасности организации, выявленных специалистом по безопасности ЗАО «Компьютерные технологии».*Перечень угроз**Угрозы утечки информации по техническим каналам** Изменения тока потребления, обусловленные обрабатываемыми техническими средствами информативными сигналами
* Радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств.
* Сбой системы кондиционирования воздуха.
* Установка непроверенных технических средств или замена вышедших из строя аппаратных компонент на неидентичные компоненты.

*Угрозы несанкционированного доступа** Наводки информативного сигнала, обрабатываемого техническими средствами, на провода и линии, выходящие за пределы контролируемой зоны предприятия, в том числе на цепи заземления и электропитания.
* Внешний нарушитель может выдавать себя за легального пользователя путем подделывания адресов в заголовках сетевых пакетов либо информации канального уровня.
* Использование недекларированных возможностей в ПО, оставленных для отладки либо умышленно внедренных.
* Внедрение несанкционированного, непроверенного или вредоносного программного кода (вирусов, троянских программ и т.п.).

*Угрозы недоступности ИТ сервисов и разрушения (утраты) информационных активов** «Маскарад» (присвоение идентификатора пользователя), использование чужих пользовательских идентификаторов, раскрытие паролей и другой аутентификационной информации.
* Атаки на отказ в обслуживании против внешних хостов компании.
* Запыление.
* Акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации.
* Нарушение безопасности по причине несоблюдения операционных процедур.
* Использование ошибок проектирования, кодирования либо конфигурации ПО.
 |

**Вариант 2**

1. Тест.

2. В Федеральном агентства железнодорожного транспорта и подведомственных ему предприятиях и учреждениях руководством составлен перечень сведений конфиденциального характера. Классифицируйте данную защищаемую информацию по видам тайны и степеням конфиденциальности.

*Перечень сведений конфиденциального характера*

* Сведения, содержащие показатели государственного оборонного заказа в
части, не содержащей сведений, составляющих государственную тайну.
* Сведения, содержащиеся в материалах служебной проверки (расследования), до утверждения акта (заключения) по проверке, а также если сведения, полученные в результате проверки (расследования), могут быть использованы в дальнейшем для противоправного действия (нанесения ущерба).
* Сведения о персональных данных работника Росжелдора, содержащиеся в личном деле работника.
* Протоколы заседаний конкурсных комиссий по проведению конкурсов на замещение вакантных должностей государственной гражданской службы.
* Сведения о штатном расписании Росжелдора.
* Сведения о расположении структурных подразделений в здании.
* Акты проверок обеспечения пропускного режима в административное здание Росжелдора.
* Сведения, содержащиеся в планах обеспечения транспортной безопасности объекта транспортной инфраструктуры и транспортного средства.
* Сведения о методах, средствах или эффективности (состоянии защиты) конфиденциальной информации в автоматизированных информационных системах, средствах вычислительной техники, других технических средствах.
* Сведения, раскрывающие содержание планов и конкретных мероприятий по охране здания Росжелдора, помещений, в которых выполняются работы, хранятся материалы, ведутся переговоры конфиденциального характера.
* Сведения об управленческих решениях, планы развития, инвестиционные программы.

**Описание экзаменационного билета**

Весьтеоретический материал курса логически разделяется на части, представленные в рабочей программе:

Раздел 1. Информационная безопасность. Основные положения, понятия, определения.

Раздел 2. Общие методы обеспечения информационной безопасности

Раздел 3: Сущность и понятие защиты информации.

Раздел 4. Организация работ по защите информации

Раздел 5. Автоматизированная система как объект информационной защиты

Раздел 6. Современные средства и способы обеспечения информационной безопасности

Вопросы теста относится к материалу, охватывающему все разделы дисциплины, второй вопрос билета – разделы 3 и 4.

Практическое задание представлено задачами на классификацию угроз безопасности информации и отнесение конфиденциальной информации по видам тайн и степеням конфиденциальности на примерах виртуальных организаций.

ПРИЛОЖЕНИЕ 1. Вопросы для подготовки к экзамену

**ПАКЕТ ЭКЗАМЕНАТОРА**

**А. УСЛОВИЯ**

Экзамен проводится в форме компьютерного тестирования и устного собеседования по билетам, содержащим задачу. Каждому студенту выдается свой вариант.

**Б. КРИТЕРИИ ОЦЕНКИ**

Выполнение заданий

|  |  |
| --- | --- |
| **Действия** | **Выполнил** **(максимально****50 баллов)** |
| Ответы на вопросы теста  | 30 |
| Решение задачи:- выбор соответствующего признака классификации;- аргументация выбора;- проведение дополнительных рассуждений, в том числе ответы на дополнительные вопросы по решению задачи. | 1587 |
| Итоговое количество баллов: | 60 |
| **5 «отлично»** | 45-60 баллов |
| **4 «хорошо»** | 45-44 балла |
| **3 «удовлетворительно»** | 33-44 баллов |
| **2 «неудовлетворительно»** | 0-32 баллов |
| **Итоговая оценка***Оценка «5»* выставляется в том случае, если студент продемонстрировал высокий уровень знании и умений по всем вопросам билета. Студент точно ответил на теоретические вопросы, правильно выполнил практическое задание. Могут быть допущены недочеты в определении понятий или при решении задачи, исправленные студентом самостоятельно в процессе ответа.*Оценка «4»* выставляется в том случае, если студент продемонстрировал понимание основного содержания теоретических вопросов, но допустил незначительные ошибки. Допущена 1 ошибка при решении задачи, исправленная студентом с помощью преподавателя.*Оценка «3»* выставляется в том случае, если студент продемонстрировал понимание основного содержания теоретических вопросов, но допустил ошибки. Могут быть допущены 2 ошибки при решении задачи, исправленные студентом с помощью преподавателя.*Оценка «2»* выставляется в том случае, если студент продемонстрировал не понимание основного содержания теоретических вопросов. Присутствуют фрагментарность, нелогичность изложения. Не решена задача. |

Количество вариантов (пакетов) заданий для студентов: 22 экзаменационных билетов.

Время выполнения задания:

*первый этап* (подготовка к ответу на теоретические вопросы) – 30 мин,

*второй этап* (выполнение практического задания) – 30 мин.
Условия выполнения заданий:

*Задания выполняются в учебной аудитории.*

*Требования охраны труда*: инструктаж по технике безопасности при работе в компьютерном классе.

*Оборудование:* персональные компьютеры, комплект лицензионного программного обеспечения.

**Литература для учащегося:**

1. Мельников В.П. Информационная безопасность : учеб. пособие для спо / В.П. Мельников, С.А. Клейменов, А.М. Петраков ; под ред. С.А. Клейменова. - 4-е изд., стереотип. - М. : Академия, 20010.
2. Анин Б.Ю. Защита компьютерной информации. Петербург, 2009. - 384с.
3. Анисимова И.Н., Стельмашонок Е.В. Защита информации. Учебное пособие. - 2009.
4. Галатенко В.А., Барсуков В.С., Водолазний В.В. Современные технологии безопасности. - М.: «Нолидж», 2009. - 496 с.

**Разработчики:**

ОГБПОУ СмолАПО \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ромашкова И.А.

преподаватель

**Экзаменационные вопросы**

1. Состояние информационной безопасности Российской Федерации и основные задачи по ее обеспечению.
2. Структура информационной безопасности и определение понятия «информационная безопасность».
3. Значение информационной безопасности для субъектов информационных отношений.
4. Национальные интересы Российской Федерации в информационной сфере и их обеспечение.
5. Принципы обеспечения информационной безопасности.
6. Концепция комплексной системы защиты информации.
7. Концептуальная модель безопасности информации.
8. Современные походы к понятию угроз защищаемой информации.
9. Классификация угроз информационной безопасности предприятия.
10. Угрозы конфиденциальной информации предприятия.
11. Случайные угрозы.
12. Преднамеренные угрозы.
13. Информация, как предмет защиты.
14. Требования, предъявляемые к защите информации.
15. Виды собственного обес­печения системы защиты информации.
16. Понятие системы защиты информации.
17. Направления защиты информации.
18. Характеристика защитных действий.
19. Понятие целей защиты информации.
20. Понятие защиты информации в компьютерных системах.
21. Этапы работы по определению и выявлению состава защищаемой информации.
22. Методика определения состава защищаемой информации.
23. Понятие «носитель защищаемой информации».
24. Носители информации как конечные объекты защиты.
25. Методика выяв­ления со­става носителей защищаемой информации.
26. Содержание концепции защиты информации в СВТ и АС.
27. Становление и развитие государственной концепции защиты информации.
28. Современная стратегия защиты информации.
29. Проблемы защиты информации.
30. Общие сведения о способах защиты информации.
31. Характеристика способов воздействия на информацию.
32. Угрозы информационным ресурсам.
33. Меры, необходимые для обеспечения безопасности сети.
34. Понятие защищаемой информации.
35. Сущность коммерческой тайны и необходимость ее защиты.
36. Органы добывания коммерческой информации.
37. Источники добывания коммерческой информации.
38. Степени секретности сведений, отнесенных к государственной тайне.
39. Структура перечней сведений, относимых к различным видам тайны.
40. Разновидности профессиональной тайны.
41. Способы пресечения разглашения конфиденциальной информации.
42. Факторы и обстоятельства, способствующие утечке информации по техническим каналам.
43. Способы несанкционированного доступа.
44. Состав и характеристика средств защиты от несанкционированного доступа.
45. Направления и средства защиты информации от HCД.
46. Парольная защита операционных систем.
47. Общие сведения о биометрических системах.
48. Параметры биометрических систем.