ПРИЛОЖЕНИЕ 1

к рабочей программе дисциплины

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ

УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«РЯЗАНСКИЙ ГОСУДАРСТВЕННЫЙ РАДИОТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

 ИМЕНИ В.Ф. УТКИНА»

Факультет вычислительной техники

Кафедра «Информационная безопасность»

**ОЦЕНОЧНЫЕ МАТЕРИАЛЫ**

по дисциплине

**Б1.Б.38 «Защита программ и данных »**

Специальность: 10.05.01 Компьютерная безопасность

Специализация: № 8 Информационная безопасность объектов информатизации

 на базе компьютерных систем в защищенном исполнении

ОПОП по специальности:

Компьютерная безопасность

Квалификация выпускника: специалист по защите информации

Форма обучения - очная

Срок обучения — 5,5 лет

Рязань 2020 г.**1 ОБЩИЕ ПОЛОЖЕНИЯ**

Оценочные материалы – это совокупность учебно-методических материалов (практических заданий, описаний форм и процедур проверки), предназначенных для оценки качества освоения обучающимися данной дисциплины как части ОПОП.

Цель – оценить соответствие знаний, умений и владений, приобретенных обучающимся в процессе изучения дисциплины, целям и требованиям ОПОП в ходе проведения промежуточной аттестации.

Основная задача – обеспечить оценку уровня сформированности общекультурных и профессиональных компетенций.

Контроль знаний обучающихся проводится в форме промежуточной аттестации.

Промежуточная аттестация проводится в виде зачета c оценкой, курсовой работы и экзамена. Форма проведения - тестирование, письменный опрос по теоретическим вопросам, выполнение практических заданий, защита курсовой работы.

**2 ПАСПОРТ ОЦЕНОЧНЫХ МАТЕРИАЛОВ ПО ДИСЦИПЛИНЕ**

|  |  |  |  |
| --- | --- | --- | --- |
| **№ п/п** | **Контролируемые разделы (темы) дисциплины** | **Код контролируемой компетенции (или её части)** | **Вид, метод, форма оценочного мероприятия** |
|
| 1 | 2 | 3 | 4 |
| 1. | Модели распространения и лицензирования ПО | ОПК-5, ПК-5, ПК-17  | Экзамен |
| 2. | Защита программного обеспечения | ОПК-5, ПК-5, ПК-17 | Экзамен |
| 3. | Защита данных | ОПК-5, ПК-5, ПК-17 | Экзамен |
| 4. | Программные и программно-технические средства защиты программ и данных | ОПК-5, ПК-5, ПК-17 | Экзамен |

**3 ОПИСАНИЕ ПОКАЗАТЕЛЕЙ И КРИТЕРИЕВ ОЦЕНИВАНИЯ**

 **КОМПЕТЕНЦИЙ**

Сформированность каждой компетенции (или ее части) в рамках освоения данной дисциплины оценивается по трехуровневой шкале:

1. пороговый уровень является обязательным для всех обучающихся по завершении освоения дисциплины;
2. продвинутый уровень характеризуется превышением минимальных характеристик сформированности компетенций по завершении освоения дисциплины;
3. эталонный уровень характеризуется максимально возможной выраженностью компетенций и является важным качественным ориентиром для самосовершенствования.

**Уровень освоения компетенций, формируемых дисциплиной:**

**Описание критериев и шкалы оценивания тестирования:**

|  |  |
| --- | --- |
| **Шкала оценивания** | **Критерий** |
| 3 балла(эталонный уровень) | уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 85 до 100% |
| 2 балла(продвинутый уровень) | уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 70 до 84% |
| 1 балл(пороговый уровень) | уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 50 до 69% |
| 0 баллов | уровень усвоения материала, предусмотренного программой: процент верных ответов на тестовые вопросы от 0 до 49% |

**Описание критериев и шкалы оценивания теоретического вопроса:**

|  |  |
| --- | --- |
| **Шкала оценивания** | **Критерий** |
| 3 балла(эталонный уровень) | выставляется студенту, который дал полный ответ на вопрос, показал глубокие систематизированные знания, смог привести примеры, ответил на дополнительные вопросы преподавателя |
| 2 балла(продвинутый уровень) | выставляется студенту, который дал полный ответ на вопрос, но на некоторые дополнительные вопросы преподавателя ответил только с помощью наводящих вопросов |
| 1 балл(пороговый уровень) | выставляется студенту, который дал неполный ответ на вопрос в билете и смог ответить на дополнительные вопросы только с помощью преподавателя |
| 0 баллов | выставляется студенту, который не смог ответить на вопрос |

На промежуточную аттестацию (экзамен) выносится тест и два теоретических вопроса. Максимально обучающийся может набрать 6 баллов. Итоговый суммарный балл студента, полученный при прохождении промежуточной аттестации, переводится в традиционную форму по системе «отлично», «хорошо», «удовлетворительно» и «неудовлетворительно».

**Оценка «отлично»** выставляется студенту, который набрал в сумме 6 баллов (выполнил все задания на эталонном уровне). Обязательным условием является выполнение всех предусмотренных в течение семестра лабораторных работ.

**Оценка «хорошо»** выставляется студенту, который набрал в сумме от 4 до 5 баллов при условии выполнения всех заданий на уровне не ниже продвинутого. Обязательным условием является выполнение всех предусмотренных в течение семестра лабораторных работ.

**Оценка «удовлетворительно»** выставляется студенту, который набрал в сумме 3 балла. Обязательным условием является выполнение всех предусмотренных в течение семестра лабораторных работ.

**Оценка «неудовлетворительно»** выставляется студенту, который набрал в сумме менее 3 баллов или не выполнил всех предусмотренных в течение семестра лабораторных работ.

4 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

**4.1. Промежуточная аттестация в форме экзамена**

|  |  |
| --- | --- |
| **Код компетенции** | **Результаты освоения ОПОП****Содержание компетенций** |
| ОПК-5 | Способность использовать нормативные правовые акты в своей профессиональной деятельности |

**Типовые практические задания (тест):**

**Вопрос 1**

Брешь в системе безопасности некой программы – это место в программном коде, которое теоретически или реально может … (закончите фразу, выбрав наиболее точное продолжение)

**Ответ:**

 **(1) (+)** быть использовано для несанкционированного доступа к управлению этой программой

 **(2)** привести к ошибкам в работе этой программы

 **(3)** вызвать неустранимую ошибку и повредить операционную систему

 **(4)** вызвать неустранимую ошибку и повредить аппаратное обеспечение компьютера

**Вопрос 2**

Что такое заплата (патч)? Выберите наиболее точный ответ

**Ответ:**

 **(1)** программный код, устраняющий уязвимость в другой программе

 **(2) (+)** программный код, используемый для модификации используемой программы

 **(3)** утилита, обновляющая версию программы

 **(4)** программа, устраняющая последствия в системе, вызванные ошибкой в работе некой другой программы

**Вопрос 3**

Куда попадает сознательная рассылка по электронной почте троянских программ под Статью 146 Уголовного Кодекса Российской Федерации "Нарушение авторских и смежных прав"?

**Ответ:**

 **(1)** под Статью 146 Уголовного Кодекса Российской Федерации "Нарушение авторских и смежных прав"?

 **(2)**   (+) под Статью 273 Уголовного Кодекса Российской Федерации "Создание, использование и распространение вредоносных программ для ЭВМ"?

**Вопрос 4**

Попадает ли сознательная рассылка по электронной почте вирусов, вызывающих DDoS-атаку, под Статью 272 Уголовного Кодекса Российской Федерации "Неправомерный доступ к компьютерной информации"?

**Ответ:**

 **(1) (+)** да

 **(2)** нет

**Вопрос 5**

Попадает ли сознательная рассылка по электронной почте троянских программ под Статью 273 Уголовного Кодекса Российской Федерации "Создание, использование и распространение вредоносных программ для ЭВМ"?

**Ответ:**

 **(1) (+)** да

 **(2)** нет

**Вопрос 6**

К какой категории охраняемой информации относится врачебная тайна?

**Ответ:**

 **(1)** государственная тайна

 **(2)** служебная тайна

 **(3) (+)** профессиональная тайна

 **(4)** объекты авторского права

**Вопрос 7**

Кто контролирует защиту конфиденциальной информации, не являющейся персональными данными и государственной тайной?

**Ответ:**

 **(1) (+)** собственник информационных ресурсов

 **(2)** государство

 **(3)** коммерческая организация по защите авторских прав

 **(3)** некоммерческая организация по защите авторских прав

 **(3)** организация, где хранится и обрабатывается информация

**Вопрос 8**

Целью вирусной (троянской)0 атаки часто становится такая конфиденциальная информация как … (выберите все правильные варианты ответа, которыми можно продолжить фразу)

**Ответ:**

 **(1) (+)** номера кредитных карт

 **(2)** серийные номера различных программ

 **(3) (+)** пароли

 **(4)** файлы  с электронными книгами

 **(5)** исполняемыефайлы ОС

 **(6) (+)** файлы  с данными пользователей

**Вопрос 9**

Что такое ботнет? Выберите наиболее точный ответ

**Ответ:**

 **(1)** группа компьютеров, зараженных одним вирусом (в том числе разными модификациями одного вируса)

 **(2) (+)** группа компьютеров, которыми с помощью вирусной атаки централизованно и удаленно управляет злоумышленник

 **(3)** группа компьютеров, объединенных в одну сеть, с помощью которых производится несанкционированная рассылка спама

 **(4)** группа компьютеров, объединившихся в одну сеть с целью заманить злоумышленника, рассылающего вирусы

**Вопрос 10**

Какой метод использовал червь Морриса для проникновения на компьютер-жертву? Выберите все правильные варианты

**Ответ:**

 **(1)** используя ошибки в системе безопасности операционной системы Microsoft Windows

 **(2)** используя ошибки в системе безопасности операционной системы MS DOS

 **(3) (+)** используя ошибки в системе безопасности операционной системы Unix

 **(4) (+)** подбор пароля

 **(5)** маскировку под полезную утилиту, которую введенный в заблуждение пользователь устанавливал самостоятельно

**Типовые теоретические вопросы:**

1. Лицензирование ПО.

2. Свободное и несвободное ПО.

3. Программы и виды права (авторское, информационное, вещное).

4. Свободное ПО - признаки и разновидности свободного ПО.

5. Несвободное, бесплатное, некоммерческое ПО.

6. Особенности защиты коммерческого ПО.

7. Направления защиты программ.

8. Классификация средств атаки на средства защиты ПО.

9. Классификация методов защиты ПО.

10. Построение технической защиты ПО от несанкционированного копирования (НСК).

11. Защита программ от НСД и НСК с помощью регистрационных кодов.

12. Защита программ от НСД и НСК с помощью навесных защит (протекторов).

14. Защита ПО от НСД и НСК с помощью электронных ключей.

|  |  |
| --- | --- |
| **Код компетенции** | **Результаты освоения ОПОП****Содержание компетенций** |
| ПК-5 | Способность участво­вать в разработке и конфигурировании программно-аппарат­ных средств защиты информации, включая защищенные опера­ционные системы |

**Типовые практические задания (тест):**

**Вопрос 1**

Каким образом проникал на компьютер первый ICQ-червь?

**Ответ:**

 **(1)** пользователю маршрутом ICQ под видом фотографий приходил зараженный файл

 **(2) (+)** пользователю приходило приглашение зайти на некий сайт, при посещении которого через уязвимость в браузере Internet Explorer и происходило заражение

 **(3)** используя уязвимость в программе, ответственной за показ баннеров в окнах клиента ICQ

 **(4)** рассылал предложение загрузить пакет обновлений для ICQ, который на самом деле оказывались вирусами

**Вопрос 2**

Вирус – это программа, способная… (продолжите фразу, выбрав наиболее точный вариант)

**Ответ:**

 **(1)** создавать свои экземпляры (обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению

 **(2) (+)** создавать свои экземпляры (не обязательно совпадающие с оригиналом) и внедрять их в вычислительные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению

 **(3)** нанести какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети

 **(4)** нанести какой-либо вред компьютеру, на котором она запускаются, или другим компьютерам в сети: прямо или посредством других программ и/или приложения

**Вопрос 3**

Что такое метаморфизм вируса? Выберите наиболее точное определение

**Ответ:**

 **(1)** метод маскировки от антивирусов с помощью шифрования

 **(2)** метод маскировки от антивирусов с помощью многоуровневого архивирования и запаковки

 **(3)** создание вирусных копий путем шифрования части кода и/или вставки в код файла дополнительных, ничего не делающих команд

 **(4) (+)** создание вирусных копий путем замены некоторых команд на аналогичные, перестановки местами частей кода, вставки между ними дополнительных, ничего не делающих команд

**Вопрос 4**

Сетевой червь – это … (продолжите фразу, выбрав наиболее точный вариант)

**Ответ:**

 **(1) (+)** вредоносная программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению систем защиты компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, не обязательно совпадающих с оригиналом

 **(2)** вредоносная программа, распространяющаяся по сетевым каналам и способная к самостоятельному преодолению систем защиты компьютерных сетей, а также к созданию и дальнейшему распространению своих копий, совпадающих с оригиналом

 **(3)** вредоносная программа, распространяющаяся по сетевым каналам и способная установить на чужом компьютере некую троянскую программу

 **(4)** вредоносная программа, распространяющаяся по сетевым каналам и способная проникнуть на чужой компьютер для выполнения ряда заложенных автором функций. Механизм размножения для сетевых червей не предусмотрен

**Вопрос 5**

В чем состоит главное отличие трояна от классического вируса или червя?

**Ответ:**

 **(1)** в способности к саморазмножению

 **(2) (+)** в неспособности к саморазмножению

 **(3)** в способности к самораспространению с использованием сетевых каналов

 **(4) (+)** в способности маскировки под легальную программу

 **(5)** в способности отложить на заданный автором срок выполнение заложенных вредоносных функций

**Вопрос 6**

Троян (троянский конь) – это программа… (продолжите фразу, выбрав наиболее точный вариант)

**Ответ:**

 **(1)** основной целью которой является незаметное проникновение в другую компьютерную систему

 **(2) (+)** основной целью которой является вредоносное воздействие по отношению к компьютерной системе

 **(3) (+)** основной целью которой является кража конфиденциальной информации

 **(4)** основной целью которой является обеспечение незаметного заражения вирусом или червем другой компьютерной системы

**Вопрос 7**

Что нужно сделать вредоносной программе, чтобы запускаться при каждой загрузке операционной системы? Выберите все правильные варианты

**Ответ:**

 **(1)** поместить свой исполняемый код в системную папку

 **(2)** поместить свой ярлык на Рабочий стол

 **(3)** поместить свой ярлык в раздел Пуск / Автозагрузка

 **(4)** указать путь к своему исполняемому коду в реестре HKLM\Software\Microsoft\Windows\CurrentVersion\AutoRUN

 **(5) (+)** указать путь к своему исполняемому коду в реестре HKLM\Software\Microsoft\Windows\CurrentVersion\RUN

**Вопрос 8**

Какие есть преимущества эвристического метода антивирусной проверки над сигнатурным?

**Ответ:**

 **(1)** он более надежный

 **(2)** он существенно менее требователен к ресурсам

 **(3) (+)** он не требует регулярного обновления антивирусных баз

 **(4) (+)** он позволяет выявлять новые, еще не описанные вирусными экспертами, вирусы

**Вопрос 9**

Пользователь организации загружает по протоколу HTTP файл, заархивированный и разбитый на части при помощи WinRAR 3.0 Архив защищен паролем. Может ли такой в этом случае вирус быть обнаружен антивирусным комплексом, установленным на шлюзе и выполняющим проверку HTTP-потока?

**Ответ:**

 **(1)** да

 **(2) (+)** нет

 **(3)** зависит от того, содержит ли какой-то из кусков вирус целиком

**Вопрос 10**

Какие из ниже перечисленных видов нарушителей действуют с умыслом?

**Ответ:**

 **(1)** халатные

 **(2)** манипулируемые

 **(3) (+)** саботажники

 **(4) (+)** нелояльные

 **(5) (+)** мотивируемые извне

**Типовые теоретические вопросы:**

1. Понятие РПВ. Виды РПВ.

2. Программные закладки (ПЗ) и защита от них.

3. Защита от троянов и вредоносных утилит

4. Кейлоггеры

5. Руткиты

6. Защита от вирусов.

7. Вредоносные программы для мобильных устройств.

8. Внедрение вредоносного ПО через автозагрузку (реестр и Планировщик Windows).

|  |  |
| --- | --- |
| **Код компетенции** | **Результаты освоения ОПОП****Содержание компетенций** |
| ПК-17 | Способность про­изво­дить установку, наладку, тестирова­ние и обслуживание со­временного об­щего и специаль­ного про­граммного обеспече­ния, вклю­чая опера­ционные системы, си­стемы управления ба­зами данных, сетевое программное обес­пе­чение |

**Типовые практические задания (тест):**

**Вопрос 11**

Какие из ниже перечисленных видов нарушителей действуют исходя из корыстных интересов?

**Ответ:**

 **(1)** халатные

 **(2)** манипулируемые

 **(3) (+)** саботажники

 **(4)** нелояльные

 **(5) (+)** мотивируемые извне

**Вопрос 2**

Какие из ниже перечисленных видов нарушителей относится к группе незлонамеренных нарушителей?

**Ответ:**

 **(1) (+)** халатные

 **(2) (+)** манипулируемые

 **(3)** саботажники

 **(4)** нелояльные

 **(5)** мотивируемые извне

**Вопрос 3**

Какие из ниже перечисленных видов нарушителей относится к группе злонамеренных нарушителей?

**Ответ:**

 **(1)** халатные

 **(2)** манипулируемые

 **(3) (+)** саботажники

 **(4) (+)** нелояльные

 **(5) (+)** мотивируемые извне

**Вопрос 4**

Какие нарушители правил хранения конфиденциальной информации относятся к типу "мотивированные извне"?

**Ответ:**

 **(1) (+)** сотрудники специально устроенные на работу для похищения информации

 **(2) (+)** подкупленные или запуганные сотрудники

 **(3)** сотрудники, стремящиеся нанести вред компании из-за личных мотивов

**Вопрос 5**

Против нарушителей правил хранения конфиденциальной информации какого типа действенными являются простые технические средства предотвращения каналов утечек - контентная фильтрация исходящего трафика в сочетании с менеджерами устройств ввода-вывода?

**Ответ:**

 **(1) (+)** халатные

 **(2)** мотивируемые извне

 **(3)** саботажники

 **(4)** нелояльные

**Вопрос 6**

Какой вид нарушителей правил хранения конфиденциальной информации совершают их, действуя из лучших побуждений?

**Ответ:**

 **(1) (+)** халатные

 **(2) (+)** манипулируемые

 **(3)** саботажники

 **(4)** нелояльные

 **(5)** мотивируемые извне

**Вопрос 7**

Выберите из приведенного списка только стандартные для Microsoft Windows NT-подобной операционной системы системные процессы:

**Ответ:**

 **(1) (+)** explorer.exe

 **(2) (+)** svchost.exe

 **(3) (+)** lsass.exe

 **(4)** anvir.exe

 **(5)** postserv.exe

 **(6) (+)** services.exe

**Вопрос 8**

Допустим Вы обнаружили подозрительную сетевую активность. С помощью каких из перечисленных утилит можно определить имя процесса, который эту активность инициировал?

**Ответ:**

 **(1)** msconfig.exe

 **(2)** internat.exe

 **(3)** netstat.exe

 **(4)** arp.exe

 **(5) (+)** tcpview.exe

 **(6)** ipconfig.exe

**Вопрос 9**

Укажите описание, соответствующее маске свойств Tripwire a

**Ответ:**

 **(1) (+)** последнее время доступа

 **(2)** создать/изменить время

 **(3)** блоки с выделенной памятью

 **(4)** устройство id, на котором находится inode

 **(5)** номер inode

 **(6)** групповой id владельца файла

**Вопрос 0**

Для чего используется опция командной строки md5sum -c?

**Ответ:**

 **(1)** читает файлы в текстовом режиме

 **(2) (+)** проверяет суммы md5 в соответствии с заданным списком

 **(3)** читает файлы в двоичном режиме

**Типовые теоретические вопросы:**

1. Программные средства резервного копирования

2. Программные средства восстановления данных:

3. Программные средства восстановления разделов жесткого диска:

4. Программные средства защиты данных от утечки (DLP).

5. Средства ОС для шифрования данных/

6. Электронный замок (аппаратный модуль доверенной загрузки).

7. Средства безопасной аутентификации.

8. СЗИ SecretNet (SecretNet Studio) и Страж.

9. Программные средства контроля целостности программ и данных.

10. Программные средства генерации паролей.

Составил

к.т.н., доцент кафедры

«Информационная безопасность» \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Ю.М. Кузьмин

Заведующий кафедрой

«Информационная безопасность»

к.т.н., доцент \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ В.Н. Пржегорлинский