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.О.37 «Программно-аппаратные средства защиты информации»

Специальность: 10.05.03 Информационная безопасность автоматизированных систем

Специализация: № 8 Разработка автоматизированных систем в защищенном исполнении

Квалификация выпускника: - специалист по защите информации

Форма обучения - очная

Срок обучения — 5,5 лет

Рязань 2021 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 с 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.	Общие вопросы ОБИ и дисциплины ПАСЗИ	ОПК-11 (ОПК-11.1; ОПК-11.2)	Зачет
2.	Защита от РПВ (ПМВ)	ОПК-11 (ОПК-11.1; ОПК-11.2)	Зачет
3.	Направления и методы защиты данных	ОПК-11 (ОПК-11.1; ОПК-11.2)	Экзамен
4.	Направления и методы защиты программ	ОПК-11 (ОПК-11.1; ОПК-11.2)	Экзамен
	Программные и программно-технические средства защиты информации	ОПК-11 (ОПК-11.1; ОПК-11.2)	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 дополни-

	тельные 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

Описание критериев и шкалы оценивания практического задания:

Шкала оценивания	Критерий
3 балла (эталонный уровень)	Задача решена верно
2 балла (продвинутый уровень)	Задача решена верно, но имеются неточности в логике решения
1 балл (пороговый уровень)	Задача решена верно, с дополнительными наводящими вопросами преподавателя
0 баллов	Задача не решена

На промежуточную аттестацию (зачет, 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 практических заданий.

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 практических заданий.

Оценка «удовлетворительно» выставляется студенту, который набрал в сумме 3 балла.

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

4 ТИПОВЫЕ КОНТРОЛЬНЫЕ ЗАДАНИЯ ИЛИ ИНЫЕ МАТЕРИАЛЫ

4.1. Промежуточная аттестация в форме зачета

Код компетенции	Результаты освоения ОПОП Содержание компетенций
ОПК-11 (ОПК-11.1; ОПК-11.2)	ОПК-11: Способен разрабатывать компоненты систем защиты информации автоматизированных систем ОПК-11.1 Выбирает программно-аппаратные средства защиты информации для использования в составе автоматизированных систем ОПК-11.2 Применяет программно-аппаратные средства защиты информации для обеспечения безопасности информации в автоматизированных системах

Типовые практические задания (тест):

Вопрос 1.
Дайте определение понятия «Угроза»:

1) это умышленное нарушение правил работы с информацией, приводящее к нарушению ущерба;
2) совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности;
3) явление, действие или процесс, результатом которого могут быть утечка, искажение, уничтожение защищаемой информации, блокирование доступа к ней;
4) непреднамеренное или несанкционированное воздействие на защищаемую информацию

Ответ:2

Вопрос 2
Ресурсы, которые подлежат защите это:

1) Активы
2) Акцизы
3) Прибыль

Ответ:1

Вопрос 3.
Какие угрозы относят к конкретным (специфическим) нарушениям безопасности :

1) угроза потери конфиденциальности
2) угроза потери целостности
3) угроза потери доступности
4) все варианты верны

Ответ: 4

Вопрос 4. По каким параметрам осуществляется Контроль целостности в СЗИ «Dallas Lock 8.0» :

1) по контрольной сумма данных, содержащихся в файле
2) по наличию файла
3) по длине файла
4) по дате и времени последней модификации

Ответ:1

Вопрос 5. Особенностью СГУ Blanco является

1) глобальное уничтожение информации на томах жестких дисков и гибких магнитных дисков;
2) протоколирование всех действий по уничтожению информации
3) многократное и комбинированное выполнение функций затирания

4) Дополнительная проверка оборудования, при помощи S.M.A.R.T. теста, для получения информации о памяти, процессоре, материнской плате, координатно – указательных устройствах, дисплее, дисководе, клавиатуре и жестком диске

Ответ:4

Вопрос 6. Отправитель А хочет внести в сообщениие m некоторую закрытую информацию k_A и передать сообщение получателю В, где P_B – идентификатор абонента B:. Как будет выглядеть электронная подпись?

1) $SIG\{k_A, [m, P_B]\}$.
2) $SIG\{[k_A m, P_B]\}$
3) $SIG\{k_A, [m, P_B]\}$.
4) $SIG\{[m, k_A P_B]\}$.

Ответ:1

Вопрос 7. Верно ли утверждение: «Самый простой и быстрый способ на основе сканирования это имитация атак»

Ответ: Не верно

Типовые теоретические вопросы:

1. Взаимосвязь понятий: защищенность, уязвимость, угроза, нарушитель, атака, ущерб, риск.
2. Виды программно-аппаратных (программно-технических) средств защиты информации.
3. Отличия программно-технических от технических средств защиты информации.
4. Каналы утечки компьютерной информации: защищаемые элементы; источники угроз; основные каналы утечки информации и средства их образования.
5. Понятие РПВ. Виды РПВ.
6. Программные закладки (ПЗ): понятие ПЗ; виды ПЗ; модели работы (воздействия на компьютерные системы) ПЗ на компьютеры; защита от программных закладок (поиск недокументированных (недекларированных) возможностей); понятие изолированной программной среды и изолированного компьютера; контроль отсутствия НДВ.
7. Защита от троянов и вредоносных утилит: утилиты скрытого администрирования (backdoor), exploit'ы, rootkit'ы и просто трояны; кейлоггеры; руткиты (руткиты уровня пользователя, руткиты уровня ядра).
8. Защита от троянов и руткитов.
9. Защита от вирусов: понятие вируса; классификация вирусов; файловые вирусы;. макровирусы; сетевые вирусы (черви); почтовые вирусы; загрузочные вирусы; методы защиты вирусов от обнаружения; вредоносные утилиты, специальные упаковщики и парольные взломщики; антивирусное ПО; методы защиты от вирусов и ПЗ; белый и черный ящики (Blacklisting и Whitelisting).
10. Вредоносные программы для мобильных устройств.
11. Внедрение вредоносного ПО через автозагрузку (реестр и Планировщик Windows): как устроен реестр; ключи автозагрузки; описание (определение) возможностей разных вариантов автозапуска программ; планировщик заданий в Windows.
12. Направления и методы защиты данных:
13. Программные средства резервного копирования (Acronis Backup).
14. Программные средства восстановления:

4.2. Промежуточная аттестация в форме экзамена

Код компетенции	Результаты освоения ОПОП Содержание компетенций
ОПК-11 (ОПК-11.1; ОПК-11.2)	ОПК-11: Способен разрабатывать компоненты систем защиты информации автоматизированных систем ОПК-11.1 Выбирает программно-аппаратные средства защиты информации для использования в составе автоматизированных систем ОПК-11.2 Применяет программно-аппаратные средства защиты информации для обеспечения безопасности информации в автоматизированных системах

Типовые практические задания (тест):

Вопрос 1. Вставьте пропущенное слово. _____локальное (однокомпонентное) или функционально-распределенное программное (программно-аппаратное) средство (комплекс), реализующее контроль за информацией, поступающей в автоматизированную систему и (или) выходящей из автоматизированной системы

1) Межсетевой экран
2) Криптомаршрутизатор
3) Средство криптографической защиты информации
4) Аппаратно-программный комплекс криптографической защиты

Ответ:1

Вопрос 2. Верно ли утверждение: «Межсетевые экраны прикладного уровня, или прокси-экраны, представляют собой программные пакеты, базирующиеся на операционных системах общего назначения»?

Ответ: Верно

Вопрос 3. Что представляет из себя устройство безопасной аутентификации eToken GT:

1) смарт-карты и USB-ключи, являющиеся полнофункциональными аналогами смарт-карт с малым объемом памяти
2) USB-ключи, сочетающие в себе возможности смарт-карт и USB флэш-накопителей
3) аппаратный генератор одноразовых паролей
4) программный генератор одноразовых паролей

Ответ: 1

Вопрос 4. Программно-аппаратное средство предназначено для решения задач:

1) идентификация пользователей при помощи персональных идентификаторов и криптографическую аутентификацию пользователей до загрузки ОС
2) обеспечения защиты корпоративного сайта в Интернет
3) обеспечения безопасности финансовых операций в системах дистанционного банковского обслуживания
4) предотвращения кражи паролей к онлайн-сервисам (электронные кошельки и др.) и социальным сетям

Вопрос 5. Страж NT является сертифицированным средством защиты информации от НСД по:

1) 3 классу защищенности
2) 2 классу защищенности
3) 1 классу защищенности
4) Не сертифицирован

Ответ:6

Вопрос 3. Какой из комплексов VipNet рекомендуется использовать для работы в государственных информационных системах?

1) ViPNet CUSTOM.
2) ViPNet BOX.
3) ViPNet IDS

Ответ: 2

Вопрос 7. Система обнаружения вторжений позволяет:

1) обнаружить подозрительную сетевую активность
2) выявить известные инструменты для анализа и взлома сетей, используемые злоумышленником
3) блокировать вредоносный трафик
4) перезапустить потенциально вредоносное соединение клиент-сервер
5) отключать атакующие устройства

Ответ: 1,2

Вопрос 8. Для каких задач предназначена система КриптоПро CSP?

1) для защиты ПК и переписки индивидуальных пользователей и организаций от несанкционированного доступа.
2) для обеспечения аутентичности, конфиденциальности и имитозащиты соединений по протоколу TLS
3) для контроля целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений правильности функционирования
4) для шифрования электронной почты

Ответ:2,3

Типовые теоретические вопросы:

1. Направления защиты программ.
2. Классификация средств атаки на средства защиты ПО.
3. Классификация методов защиты ПО:
4. Построение технической защиты ПО от несанкционированного копирования (НСК):
5. Защита программ от НСД и НСК с помощью регистрационных кодов:
6. Защита программ от НСД и НСК с помощью навесных защит (протекторов):
7. Защита ПО от НСД и НСК с помощью электронных ключей:
8. Электронный замок (аппаратный модуль доверенной загрузки) «Соболь».
9. Средства безопасной аутентификации типа RuToken.
10. СЗИ SecretNet (SecretNet Studio) и Страж.
11. Программные средства генерации паролей.
12. Программные средства анализа защищенности сети (Ревизор).
13. Программные средства защиты данных от утечки:
14. Средства шфрования данных:
15. Средства гарантированного уничтожения (затирания) данных:
16. Программные средства контроля целостности программ и данных.

Составил
к.т.н., доцент кафедры
«Информационная безопасность» _____ Ю.М. Кузьмин

Заведующий кафедрой
«Информационная безопасность»
к.т.н., доцент _____ В.Н. Пржегорлинский