МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Воронежский государственный технический университет»

УТВЕРЖДАЮ
Декан факультета _____ С.М. Пасмурнов
«31» августа 2017 г.

РАБОЧАЯ ПРОГРАММА

дисциплины

«Защита программ и данных»

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2016

Автор программы _____/В.Н. Деревянко/

Заведующий кафедрой
Систем информационной
безопасности _____/ А.Г. Остапенко /

Руководитель ОПОП _____/ А.Г. Остапенко /

Воронеж 2017

1.ЦЕЛИИЗАДАЧИДИСЦИПЛИНЫ

1.1.Целидисциплины

Формирование навыков ценностно-информационного подхода к защите программ и данных в компьютерных системах

1.2.Задачиосвоениядисциплины

- подготовить специалиста с глубокими знаниями в области основ защиты программ и данных;
- научить основным принципам обеспечения безопасности программ и данных;
- изучение методологии анализа безопасности программ и данных, тестирования программ, оценке вероятности наличия в программном обеспечении разрушающих программных средств, а также обеспечению целостности и достоверности используемого программного кода

2.МЕСТОДИСЦИПЛИНЫВСТРУКТУРЕОПОП

Дисциплина«Защитапрограммиданных»относитсякдисциплинамбазовойчастиблока Б1.

3.ПЕРЕЧЕНЬПЛАНИРУЕМЫХРЕЗУЛЬТАТОВОБУЧЕНИЯПОДИСЦИПЛИНЕ

Процессизучениядисциплины«Защитапрограммиданных»направленна формированиеследующихкомпетенций:

ОПК-8-способностьюиспользоватьязыкиисистемыпрограммирования,инструментальныесредствадлярешенияпрофессиональных,исследовательскихиприкладныхзадач

ПК-5-способностьюучаствоватьвразработкеиконфигурированиипрограммно-аппаратныхсредствзащитыинформации,включаязащищенныеоперационныесистемы,системыуправлениябазамиданных,компьютерныесети,системыантивирусной защиты,средствакриптографическойзащитыинформации

ПК-12-способностьюпроводитьинструментальныймониторингзащищенностикомпьютерныхсистем

ПК-14-способностьюорганизовыватьработыповыполнениюрежимазащитыинформации,втомчислеограниченногодоступа

ПК-19-способностьюпроизводитьпроверкитехническогосостоянияипрофилактическиеосмотрытехническихсредствзащитыинформации

Компетенция	Результатыобучения,характеризующие сформированностькомпетенции
ОПК-8	Знатьязыки и системы программирования
	Уметьиспользовать языки и системы программирования для решения профессиональных, исследовательских и прикладных задач
	Владетьинструментальными средствами для решения профессиональных, исследовательских и прикладных задач
ПК-5	Знать функционал средств защиты информации

	Уметьучаствовать в разработке и конфигурировании программно-аппаратных средств защиты информации
	Владеть доступными интерфейсами средств защиты информации
ПК-12	Знать требования к защищенности информационных систем
	Уметьпроводить инструментальный мониторинг защищенности компьютерных систем
	Владеть инструментами мониторинг защищенности компьютерных систем
ПК-14	Знать требования режима защиты информации, в том числе ограниченного доступа
	Уметьорганизовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа
	Владеть методами обеспечения режима защиты информации, в том числе ограниченного доступа
ПК-19	Знать показатели и критерии технического состояния технических средств защиты информации
	Уметьпроизводить проверки технического состояния и профилактические осмотры технических средств защиты информации
	Владеть методами и средствами проверки технического состояния и профилактические осмотры технических средств защиты информации

4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Защитапрограммиданных»составляет 3з.е.

Распределениетрудоемкостидисциплиныповидамзанятий **очнаяформаобучения**

Видыучебнойработы	Всегочасов	Семестры
		8
Аудиторныезанятия (всего)	54	54
В томчисле:		
Лекции	36	36
Лабораторныеработы (ЛР)	18	18
Самостоятельнаяработа	54	54
Видыпромежуточнойаттестации - зачет	+	+
Общая трудоемкость: академические часы зач.ед.	 108 3	 108 3

5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидамзанятий

очнаяформаобучения

№ п/п	Наименованиетемы	Содержаниераздела	Лекц	Лаб. зан.	СРС	Всего, час
1	Введение в теорию обеспечения безопасности программного обеспечения и данных	Основные положения теории безопасности программ и данных. Угрозы безопасности программному обеспечению и данным. Теоретические основы дисциплины и терминология.Основные принципы обеспечения безопасности программного обеспечения и данных. Технологическая и эксплуатационная безопасность программ	6	4	8	18
2	Методы и средства анализа безопасности программного обеспечения и данных	Контрольно-испытательные методы анализа безопасности программ и данных. Логико-аналитические методы контроля безопасности программ и данных. Сравнительный анализ логико-аналитических и контрольно-испытательных методов анализа безопасности программ и данных.Выявление уязвимостей программ и данных. Выбор программного обеспечения безопасности компьютерных систем. Модели поведения программного обеспечения.	6	4	8	18
3	Способы тестирования программного обеспечения при испытаниях его на технологическую безопасность	Обобщенные способы анализа программных средств на предмет наличия (отсутствия) разрушающих программных средств.Построение программно-аппаратных комплексов для контроля технологической безопасности программного обеспечения и данных.	6	4	8	18
4	Расчет вероятности наличия разрушающих программных средств на этапе испытаний программного обеспечения и подходы к его исследованию	Постановка задачи. Обоснование множества информационных характеристик. Алгоритмы приближенных вычислений вероятностных характеристик наличия в программном обеспечении разрушающих программных средств.Обоснование критериев принятия решений о наличии в программном обеспечении разрушающих программных средств. Подходы к исследованиюбезопасности сложных программных комплексов.	6	2	10	18
5	Методы обеспечения надежности программ для контроля их технологической безопасности	Исходные данные, определения и условия. Анализ существующих моделей надежности программного обеспечения.Модель Нельсона. Оценка технологической безопасности программного обеспечения на базе модели Нельсона.	6	2	10	18
6	Методы и средства обеспечения целостности и достоверности используемого программного кода	Методы защиты программ и данных от несанкционированных изменений. Проверка целостности программ и данных.Схема подписи с верификацией по запросу. Примеры применения схемы подписи с верификацией по запросу.Основные подходы к защите программного обеспечения от несанкционированного копирования.	6	2	10	18
		Итого	**36**	**18**	**54**	**108**

5.2Переченьлабораторныхработ

1) Оценка уязвимости программного обеспечения компьютерных систем.
2) Выбор рационального варианта средства защиты программного обеспечения компьютерных систем.

3) Формирование альтернативных вариантов комплексов средств защиты программного обеспечения компьютерных систем методом морфологического анализа.
4) Выбор рационального варианта комплекса средств защиты программного обеспечения компьютерных систем.

6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

Всоответствиисучебнымпланомосвоениедисциплинынепредусматриваетвыполнениекурсовогопроекта(работы)иликонтрольнойработы.

7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

7.1.Описаниепоказателейикритериевоцениваниякомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Аттестован	Неаттестован
ОПК-8	Знать языки и системы программирования	Знает операторы и конструкции языка	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь использовать языки и системы программирования для решения профессиональных, исследовательских и прикладных задач	Умеет применять языки и системы программирования для решения профессиональных, исследовательских и прикладных задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть инструментальными средствами для решения профессиональных, исследовательских и прикладных задач	Владеет инструментальными средствами для решения профессиональных, исследовательских и прикладных задач	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-5	Знать функционал средств защиты информации	Знает функционал основных типов и классов средств защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь участвовать в разработке и конфигурировании программно-аппаратн	Умеет разрабатывать и конфигурировать программно-аппаратные средства защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	ых средств защиты информации			
	Владеть доступными интерфейсами средств защиты информации	Владеет доступными интерфейсами средств защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-12	Знать требования к защищенности информационных систем	Знает требования к защищенности информационных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь проводить инструментальный мониторинг защищенности компьютерных систем	Умеет проводить инструментальный мониторинг защищенности компьютерных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть инструментами мониторинг защищенности компьютерных систем	Владеет инструментами мониторинг защищенности компьютерных систем	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-14	Знать требования режима защиты информации, в том числе ограниченного доступа	Знает требования режима защиты информации, в том числе ограниченного доступа	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа	Умеет организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Владеть методами обеспечения режима защиты информации, в том числе ограниченного доступа	Владеет методами обеспечения режима защиты информации, в том числе ограниченного доступа	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
ПК-19	Знать показатели и критерии технического состояния технических средств защиты информации	Знает показатели и критерии технического состояния технических средств защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах
	Уметь производить проверки технического состояния и	Умеет производить проверки технического состояния и профилактические осмотры технических	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

	профилактические осмотры технических средств защиты информации	средств защиты информации		
	Владеть методами и средствами проверки технического состояния и профилактические осмотры технических средств защиты информации	Владеет методами и средствами проверки технического состояния и профилактические осмотры технических средств защиты информации	Выполнение работ в срок, предусмотренный в рабочих программах	Невыполнение работ в срок, предусмотренный в рабочих программах

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв8семестредля очнойформыобученияподвухбалльнойсистеме:

«зачтено»

«незачтено»

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции	Критерии оценивания	Зачтено	Незачтено
ОПК-8	Знать языки и системы программирования	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	Уметь использовать языки и системы программирования для решения профессиональных, исследовательских и прикладных задач	Решениестандартныхпрактическихзадач	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены
	Владеть инструментальными средствами для решения профессиональных, исследовательских и прикладных задач	Решение прикладных задач в конкретной предметной области	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены
ПК-5	Знать функционал средств защиты информации	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	Уметь участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации	Решениестандартныхпрактическихзадач	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены
	Владеть доступными интерфейсами средств	Решение прикладных задач в конкретной предметной области	Продемонстрирована верный ход решения в большинстве задач	Задачинерешены

	защиты информации			
ПК-12	Знать требования к защищенности информационных систем	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	Уметь проводить инструментальный мониторинг защищенности компьютерных систем	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	Владеть инструментами мониторинг защищенности компьютерных систем	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
ПК-14	Знать требования режима защиты информации, в том числе ограниченного доступа	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	Уметь организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
	Владеть методами обеспечения режима защиты информации, в том числе ограниченного доступа	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены
ПК-19	Знать показатели и критерии технического состояния технических средств защиты информации	Тест	Выполнениетестана 70-100%	Выполнениеменее 70%
	Уметь производить проверки технического состояния и профилактические осмотры технических средств защиты информации	Решениестандартныхпрактическихзадач	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены

	Владеть методами и средствами проверки технического состояния и профилактические осмотры технических средств защиты информации	Решение прикладных задач в конкретной предметной области	Продемонстрирова н верный ход решения в большинстве задач	Задачинерешены

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныеза данияилииныематериалы,необходимыедляоценкизнаний,умений,навык ови(или)опытадеятельности)

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

Задание № 1

Вопрос:

Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются

Выберите один из 4 вариантов ответа:

1) пароли
2) анкеты
3) коды
4) ярлыки

Задание № 2

Вопрос:

От несанкционированного доступа может быть защищён:

Выберите несколько из 4 вариантов ответа:

1) каждый диск
2) папка
3) файл
4) ярлык

Задание № 3

Вопрос:

К биометрическим системам защиты информации относятся системы идентификации по:

Выберите несколько из 9 вариантов ответа:

1) отпечаткам пальцев
2) характеристикам речи
3) радужной оболочке глаза
4) изображению лица
5) геометрии ладони руки
6) росту
7) весу
8) цвету глаз
9) цвету волос

Задание № 4
Вопрос:
Какие существуют массивы дисков RAID?
Выберите несколько из 4 вариантов ответа:
1) RAID 0
2) RAID 1
3) RAID 10
4) RAID 20

Задание№ 5
Вопрос:
Найди соответствие.
Укажите соответствие для всех 2 вариантов ответа:
1) Для создания массива этого уровня понадобится как минимум два диска одинакового размера. Запись осуществляется по принципу чередования: данные делятся на порции одинакового размера (A1, A2, A3 и т.д.), и поочерёдно распределяются по всем дискам, входящим в массив.
2) Массивы этого уровня построены по принципу зеркалирования, при котором все порции данных (A1, A2, A3 и т.д.), записанные на одном диске, дублируются на другом.
__ RAID 0
__ RAID 1

Задание № 6
Вопрос:
Выберите типы вредоносных программ:
Выберите несколько из 6 вариантов ответа:
1) Вирусы, черви, троянские и хакерские программы
2) Шпионское, рекламное программное обеспечение
3) Потенциально опасное программное обеспечение
4) Операционная система Linux
5) Операционная система Windows

Задание № 7
Вопрос:
Найди соответствие.
Укажите соответствие для всех 2 вариантов ответа:
1) сигнатуры. Сигнатура - это некоторая постоянная последовательность программного кода, специфичная для конкретной вредоносной программы.
2) алгоритмы эвристического сканирования, т.е.анализа последовательности команд в проверяемом объекте.
__ Для поиска известных вредоносных программ используются
__ Для поиска новых вирусов используются

Задание № 8

Вопрос:

Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:

1) автоматически при старте операционной системы и работает в качестве фонового системного процессора, проверяя на вредоносность совершаемые другими программами действия. Основная задача состоит в обеспечении максимальной защиты от вредоносных программ при минимальном замедлении работы компьютера.

2) по заранее выбранному расписанию или в произвольный момент пользователем. Производит поиск вредоносных программ в оперативной памяти, а также на жестких и сетевых дисках компьютера.

__ Антивирусный монитор запускается

__ Антивирусный сканер запускается

Задание № 9

Вопрос:

Компьютерные вирусы -

Выберите один из 5 вариантов ответа:

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Задание № 10

Вопрос:

По "среде обитания" вирусы можно разделить на:

Выберите несколько из 6 вариантов ответа:

1) загрузочные

2) файловые

3) макровирусы

4) очень опасные

5) не опасные

6) опасные

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

Задание № 11

Вопрос:

Найди соответствие.

Укажите соответствие для всех 3 вариантов ответа:

1) заражают загрузочный сектор гибкого или жёсткого диска.

2) эти вирусы различными способами внедряются в исполнимые файлы и обычно активизируются при их запуске.

3) существуют для интегрированного офисного приложения MicrosoftOffice.

__ загрузочные вирусы

__ файловые вирусы

__ макровирусы

Задание № 12

Вопрос:

Сетевые черви -

Выберите один из 5 вариантов ответа:

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их

обнаружения антивирусными программами.

Задание № 13
Вопрос:
Сетевые черви бывают:
Выберите несколько из 4 вариантов ответа:
1) Web-черви
2) почтовые черви
3) черви операционной системы
4) черви MS Office

Задание № 14
Вопрос:
Найди соответствие.
Укажите соответствие для всех 2 вариантов ответа:
1) Профилактическая защита от таких червей состоит в том, что в браузере можно запретить получение активных элементов на локальный компьютер.
2) Профилактическая защита от таких червей состоит в том, что не рекомендуется открывать вложенные в сообщения файлы, полученные от сомнительных источников. А также рекомендуется своевременно скачивать из Интернета и устанавливать обновления системы безопасности операционной системы и приложений.
__ Web-черви

__ почтовые черви

Задание № 15
Вопрос:
Наиболее эффективны от Web-червей, Web-антивирусные программы, которые включают:
Выберите несколько из 3 вариантов ответа:
1) межсетевой экран
2) модуль проверки скриптов
3) антивирусный сканер

Задание № 16
Вопрос:
Межсетевой экран (брандмауэр) -
Выберите один из 5 вариантов ответа:
1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.
2) являются вредоносными программами, которые проникают на

компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Задание № 17

Вопрос:

Троянская программа, троянец -

Выберите один из 5 вариантов ответа:

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.

2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.

3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.

4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.

5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

Задание № 18

Вопрос:

Троянские программы бывают:

Выберите несколько из 4 вариантов ответа:

1) утилиты удалённого администрирования

2) программы - шпионы

3) рекламные программы

4) программы удаления данных на локальном компьютере

Задание № 19

Вопрос:

Найди соответствие.

Укажите соответствие для всех 3 вариантов ответа:

1) троянские программы данного типа являются одним из самых опасных видов вредоносного программного обеспечения, поскольку в них заложена возможность самых разнообразных злоумышленных действий, в том числе они могут быть использованы для обнаружения и передачи кофиденциальной информации.

2) троянские программы этого типа часто используются для кражи информации пользователей различных систем онлайновых платежей и банковских систем.

3) эти программы встраивают рекламу в основную полезную программу и могут выполнять функцию троянских программ. Эти программы могут скрытно собирать различную информацию о пользователе компьютера и затем отправлять её злоумышленнику.

__ Троянские утилиты удалённого администрирования

__ Троянские программы - шпионы

__ Рекламные программы

Задание № 20

Вопрос:

Найди соответствие.

Укажите соответствие для всех 2 вариантов ответа:

1) реализуют атаку с одного компьютера с ведома пользователя. Эти программы обычно наносят ущерб удалённым компьютерам и сетям, не нарушая работоспособности заражённого компьютера.

2) реализуют распределённые атаки с разных компьютеров, причём без ведома пользователей заражённых компьютеров.

__ DoS - программы

__ DDos - программы

7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач

Вопрос № 1 Предоставление определённому лицу или группе лиц прав на выполнение определённых действий, а также процесс проверки (подтверждения) данных прав при попытке выполнения этих действий называется:

А Авторизацией

Б Аутентификацией

В Идентификацией

Г Управлением доступом

Вопрос № 2 Сеть из взломанных компьютеров, на которых выполняются вредоносные программы, которая удаленно контролируется киберпреступниками и используются для DDoS-атак, рассылки спама, называется:

А Брутфорс

Б Воронка

В Упаковщик

Г Ботнет

Вопрос № 3 Обнаружение действий, направленных на НСД к информации, специальные воздействия на информацию в целях добывания, уничтожения, искажения и блокирования доступа к ней, а также реагирование на эти действия обеспечиваются:

А Антивирусной защитой

Б Обнаружением (предотвращением) вторжений

В Ограничениями программной среды.

Г Идентификацией и аутентификацией субъектов доступа и объектов доступа

Вопрос № 4 Какая была пропускная способность у самой мощной DDoS-атаки?

А Около 500 Мбит/с

Б Около 1 Гбит/с

В Около 500 Гбит/с

Г Более 1 Тбит/с

Вопрос № 5 Механизм обмана пользователя, при котором жертва думает, что щелкает по определенному объекту на странице, а на самом деле кликает по объекту, встроенному в страницу злоумышленником, называется:

А Кибersквоттинг

Б Словарная атака

В Кликджекинг

Г Поведенческий анализ

Вопрос № 6 Допустим, вы столкнулись с инцидентом в вашей сети. Что вы сделаете в первую очередь, прежде чем его исследовать?

А Изолирую систему от корпоративной сети

Б Перезапущу компьютер

В Сделаю образ диска

Г Сохраню дамп памяти

Вопрос № 7 Какие сервисы компании могут стать мишенью для DDoS-атак?

А Общедоступные сайты и порталы для клиентов

Б Серверы почты и сервисы сообщений

В Файл-серверы и сервисы, обеспечивающие транзакции

Г Все вышеперечисленное

Вопрос № 8 Что означает аббревиатура EDR?

А EpicDelayReduction (эпическое сокращение задержки) – технология, ускоряющая наиболее длительные операции

Б Это тикеркриптовалюты E-DinarCoin

В EndpointDetectionandRemediation – обнаружение атак на рабочих станциях и принятие корректирующих мер

Г EndpointDetectionandResponse – обнаружение атак на рабочих станциях и реагирование на них

Вопрос № 9 Дискреционная политика доступа:

А Определяет права доступа идентифицированных субъектов к объектам на основе заданных внешних правил (матрицы доступа)

Б Определяет права доступа субъектов к объектам или разрешает информационные потоки между объектами на основе изменяемых меток прав доступа или конфиденциальности

В Является алгоритмом формирования матрицы доступа

Г Содержит инструкцию для системного администратора по предоставлению прав доступа различным пользователям

Вопрос № 10 Программа, перехватывающая нажатия клавиш на клавиатуре и отправляющая их злоумышленникам, называется:

А Кликджекинг

Б Кейлоггер

В Кэшбэк

Г Криптор

Вопрос № 11 Какова конечная цель идентификации и аутентификации субъекта в системе?

А Его допуск к информации ограниченного пользования при положительном результате или отказ в допуске при отрицательном результате

Б Определение его принадлежности к числу пользователей или аппаратных устройств компьютера

В Определение времени, отведенного объекту (субъекту) на работу

Г Выделение объекту (субъекту) определенного объема памяти

7.2.4Примерныйпереченьвопросовдляподготовкикзачету

1. Понятие информационной безопасности. Основные составляющие информационной

безопасности.

2. Важность и сложность проблемы информационной безопасности

3. Программно-технические меры безопасности. Понятие сервиса информационной

безопасности. Архитектурная безопасность.

4. Понятие сервиса информационной безопасности. Идентификация и аутентификация.

5. Понятие сервиса информационной безопасности. Управление доступом.

6. Понятие сервиса информационной безопасности. протоколирование и аудит.

7. Понятие сервиса информационной безопасности. управление и

анализ защищенности.

8. Понятие сервиса информационной безопасности. обеспечение высокой доступности и

отказоустойчивости.

9. Понятие сервиса информационной безопасности. экранирование и туннелирование.

10. Понятие сервиса информационной безопасности. криптография: шифрование.

11. Понятие сервиса информационной безопасности. криптография: контроль

целостности.

12. Криптология : базовые понятия и терминология.

13. Криптографические примитивы и их свойства.

14. Модели основных криптоаналитических атак.

15. Антивирусная защита. История развития вирусов и их классификация. Методызащитыотвредоносныхпрограмм

7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач

Непредусмотреноучебнымпланом

7.2.6.Методикавыставленияоценкиприпроведенииипромежуточной аттестации

Зачет проводитсяпотест-билетам,каждыйизкоторыхсодержит10вопросовизадачу.Каждыйправильныйответнавопросвтестеоценивается1баллом,задачаоценивается в10баллов(5балловверноерешениеи5балловзаверныйответ).Максимальноеколичествонабранныхбаллов–20.

1.Оценка«Не зачтено»ставитсявслучае,еслистудентнабралменее6баллов.

2.Оценка«Зачтено»ставитсявслучае,еслистудентнабралот6до20баллов.

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(темы) дисциплины	Кодконтролируемойкомпетенции	Наименованиеоценочногосредства
1	Знать языки и системы программирования	ОПК-8, ПК-5, ПК- 12, ПК-14, ПК-19	Тест, контрольная работа, защита лабораторных работ, защита реферата,
2	Уметь использовать языки и системы программирования для решения профессиональных, исследовательских и прикладных задач	ОПК-8, ПК-5, ПК- 12, ПК-14, ПК-19	Тест, контрольная работа, защита лабораторных работ, защита реферата,
3	Владеть инструментальными средствами для решения профессиональных, исследовательских и	ОПК-8, ПК-5, ПК- 12, ПК-14, ПК-19	Тест, контрольная работа, защита лабораторных работ, защита реферата,

	прикладных задач		
4	Знать функционал средств защиты информации	ОПК-8, ПК-5, ПК- 12, ПК-14, ПК-19	Тест, контрольная работа, защита лабораторных работ, защита реферата,
5	Уметь участвовать в разработке и конфигурировании программно-аппаратных средств защиты информации	ОПК-8, ПК-5, ПК- 12, ПК-14, ПК-19	Тест, контрольная работа, защита лабораторных работ, защита реферата,
6	Владеть доступными интерфейсами средств защиты информации	ОПК-8, ПК-5, ПК- 12, ПК-14, ПК-19	Тест, контрольная работа, защита лабораторных работ, защита реферата,

7.3.Методическиематериалы,определяющиепроцедурыоценивания знаний,умений,навыкови(или)опытадеятельности

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхтест-заданийнабумажномносителе.Времятестирования30мин.Затемосуществляетсяпроверкатестаэкзаменатором ивыставляетсяоценкасогласнометодикивыставленияоценкиприпроведении промежуточнойаттестации.

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценки припроведениипромежуточнойаттестации.

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномносителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязадачэкзаменаторомивыставляетсяоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестации.

8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

Основная литература:

1. Кащенко Г.А. Защита программного обеспечения от несанкционированного использования [Электронный ресурс]: Учеб.пособие / Г. А. Кащенко. - Электрон.текстовые, граф. дан. (559 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 30-00.

2. Кащенко, Г.А. Защита программ и данных [Электронный ресурс] / Г. А. Кащенко; Учеб.пособие. - Электрон.текстовые, граф. дан. (3,28 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 30-00.

3. Савинков, А.Ю. Разграничение доступа UNIX и LINUX: [Учеб.пособие] / А. Ю. Савинков. - Воронеж: ВИРО, 2016. - ISBN 978-59907345-5-5: 100-00.

Дополнительная литература:

1. Методические указания к самостоятельным работам по дисциплинам «Защита программ и данных», «Защита в операционных системах» для студентов специальности 090301 «Компьютерная безопасность» очной формы обучения [Электронный ресурс] / Каф.систем информационной безопасности; Сост. Г. А. Кащенко. - Электрон.текстовые, граф. дан. (442 Кб). - Воронеж: ФГБОУ ВПО "Воронежскийгосударственныйтехническийуниверситет", 2015. - 1 файл. - 00-00.

2. Методические указания к лабораторным работам № 5–8 по дисциплинам «Защита в операционных системах», «Безопасность операционных систем» для студентов специальностей 090301 «Компьютерная безопасность», 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф.систем информационной безопасности; Сост.: А. Ю. Савинков, Н. А. Ленков, В. Н. Деревянко. - Электрон.текстовые, граф. дан. (424 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

3. Методические указания к практическим занятиям по дисциплине «Защита в операционных системах» для студентов специальности 090301 «Компьютерная безопасность» очной формы обучения [Электронный ресурс] / Каф.систем информационной безопасности; Сост.: А. Ю. Савиков, Н. А. Ленков, В. Н. Деревянко. - Электрон.текстовые, граф. дан. (332 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2015. - 1 файл. - 00-00.

8.2Переченьинформационныхтехнологий,используемыхприосуществленииобразовательногопроцессаподисциплине,включаяперечень лицензионногопрограммногообеспечения,ресурсовинформационно-телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданныхиинформационныхсправочныхсистем:

1) Банк данных угроз безопасности информации – URL: http://bdu.fstec.ru.

2) Информационно-правовая система «Законодательство России» // Официальный интернет-портал правовой информации – URL: http://pravo.gov.ru/proxy/ips.

3) Каталог стандартов // Официальный сайт Росстандарта – URL: http://www.gost.ru/wps/portal/pages.CatalogOfStandarts.

4) Официальный сайт ФСТЭК России – URL: http://fstec.ru.

9МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯБАЗА,НЕОБХОДИМАЯДЛЯОСУЩЕСТВЛЕНИЯОБРАЗОВАТЕЛЬНОГОПРОЦЕССА

Компьютерных класс с количеством персональных компьютеров из расчета 1 персональный компьютер на 2 обучающихся.

10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Защитапрограммиданных»читаютсялекции,проводятсялабораторныеработы.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсяналиболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотражениявучебнойлитературе.

Лабораторныеработывыполняютсяналабораторномоборудованиивсоответствиисметодиками,приведеннымивуказанияхквыполнениюработ.

Видучебныхзанятий	Деятельностьстудента
Лекция	Написание конспекта лекций: кратко, схематично, последовательно фиксировать основные положения, выводы, формулировки, обобщения; помечать важные мысли, выделять ключевые слова, термины. Проверка терминов, понятий с помощью энциклопедий, словарей, справочников с выписыванием толкований в тетрадь. Обозначение вопросов, терминов, материала, которые вызывают трудности, поиск ответов в рекомендуемой литературе. Если самостоятельно не удается разобраться в материале, необходимо сформулировать вопрос и задать преподавателю на лекции или на практическом занятии.
Лабораторнаяработа	Лабораторные работы позволяют научиться применять теоретические знания, полученные на лекции при решении конкретных задач. Чтобы наиболее рационально и полно использовать все возможности лабораторных для подготовки к ним необходимо: следует разобрать лекцию по соответствующей теме, ознакомится с соответствующим разделом учебника, проработать дополнительную литературу и источники, решить задачи и выполнить другие письменные задания.
Самостоятельнаяработа	Самостоятельная работа студентов способствует глубокому усвоения учебного материала и развитию навыков самообразования. Самостоятельная работа предполагает следующие составляющие: - работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций; - выполнение домашних заданий и расчетов; - работа над темами для самостоятельного изучения; - участие в работе студенческих научных конференций, олимпиад; - подготовка к промежуточнойаттестации.
Подготовка к промежуточнойаттестации	Готовиться к промежуточной аттестации следует систематически, в течение всего семестра. Интенсивная подготовка должна начаться не позднее, чем за месяц-полтора до промежуточной аттестации. Данные перед зачетом три дня эффективнее всего использовать для повторения и систематизации материала.