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

«Системы обнаружения компьютерных атак»

Специальность 10.05.01 КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ

Специализация Безопасность распределенных компьютерных систем

Квалификация выпускника специалист по защите информации

Нормативный период обучения 5 лет и 6 м.

Форма обучения очная

Год начала подготовки 2017

Автор программы _____ /В.И. Белоножкин/

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

Руководитель ОПОП _____ / А.Г. Остапенко /

Воронеж 2017

1.1.Целидисциплины

Формирование и закрепление общепрофессиональных и профессиональных ком

1.2.Задачиосвоениядисциплины

- ознакомление с основными принципами построения систем обнаружения ко
- формирование умений анализировать защищенность компьютерных систем, адми
- приобретение навыков выявления и устранения уязвимостей компьютерн

Дисциплина«Системыобнаружениякомпьютерныхатак»относитсякдисциплинам
освоения дисциплины "Системы обнаружения компьютерных атак" требуются знания

Программа устанавливает минимальные требования к знаниям и умениям студе
виды учебных занятий и отчетности.

Программа разработана в соответствии с: Федеральным государственным образ
направлению подготовки 10.05.01 «Компьютерная безопасность», специализация "Бе

Процессизучениядисциплины«Системыобнаружениякомпьютерныхатак»направ

ОПК-3-
способностьюпониматьзначениеинформациивразвитиисовременногообщества,примен
хинформации

ПК-7-способностьюпроводитьанализпроектныхрешенийпообеспечениюзащище

ПК-16-способностьюразрабатыватьпроектынормативныхправовыхактовиметоди

ПК-20-способностьювыполнятьработыповосстановлениюработоспособностисре

ПСК-3.3-способностьюиспользоватьсовременныесредыитехнологии,разработки

ПСК-3.4-способностьюорганизовыватьзащитуинформациираспределенныхком

Компетенция	
ОПК-3	знать осн
	уметь на
	владеть н
ПК-7	знать осн
	уметь ан
	владеть н
ПК-16	знать осн
	уметь фо
	владеть н
ПК-20	знать спо
	уметь ад
	владеть
ПСК-3.3	знать нап
	уметь оце
	владеть

ПСК-3.4	знать фор
	уметь орг
	владеть н

Общаятрудоемкостьдисциплины«Системыобнаружениякомпьютерныхатак»сост
Распределениетрудоемкостидисциплиныповидамзанятий
очнаяформаобучения

Виды учебной работы	Всего часов	Семестры	
		7	8
Аудиторные занятия (всего)	108	54	54
В том числе:			
Лекции	72	36	36
Лабораторные работы (ЛР)	36	18	18
Самостоятельная работа	108	72	36
Часы на контроль	36	-	36
Виды промежуточной аттестации - экзамен, зачет	+	+	+
Общая трудоемкость: академические часы зач.ед.	 252 7	 126 3.5	 126 3.5

5.1Содержаниеразделовдисциплиныираспределениетрудоемкостиповидамз

№ п/п	Наименование темы	
1	Системный подход к обеспечению защиты от компью-терных атак	Компьют Направле Организац
2	Средства выявления и локализации уязвимостей компьютерных систем к воздействию угроз без-опасности	Методы к Методы уничтоже
3	Методы и средства обнаружения и отражения се-тевых атак	Методы к Контентн Средства
4	Комплексные системы защиты от компьютерных атак	Доверенн Подсисте Комплекс Системы Оснащени

5.2Переченьлабораторныхработ

1. Классификация и оценка необходимости защиты реальных компьютерных систем.

2. Построение алгоритмов компьютерных атак на примерах реальных инцидентов.
3. Расчет рисков компьютерной системы с помощью системыDigital Security Office.
4. Построение модели безопасности компьютерной системы.
5. Разработка нормативно-распорядительных документов для организации защиты ком
6. Тестирование программных средств для экспертных исследований следов компью
7. Исследование безопасности платформ виртуализации.
8. Анализ защищенности компьютерной системы с помощью сетевого сканера Nessus.
9. Сравнительный анализ эффективности средств контроля доступа к компьютерной
10. Настройка и исследование функций Smart UPS.
Анализ применения программных средств гарантированного удаления информации.
11. Исследование подсистемы безопасности ОС семейства Windows..
12. Исследование подсистемы безопасности ОС семейства Linux.
13. Исследование подсистемы безопасности СУБД "Линтер".
14. Настройка подсистем безопасности интернет-браузеров и почтовых клиентов.
15. Тестирование функций системы защиты ЛВС Secret Net.
16. Настройка таблицы правил межсетевого экрана.
17. Анализ эффективности систем обнаружения компьютерных атак.
18. Тестирование функций VPN-решения VipNet Client.

Всоответствиисучебнымпланомосвоениедисциплинынепредусматриваетвыполн

7.ОЦЕНОЧНЫЕМАТ

7.1.Описаниепоказателейикритериевоцениваниякомпетенцийнаразличных

7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпо
«аттестован»;
«неаттестован».

Компе- тенция	Результатыобучения,характеризующие сформированностькомпетенции
ОПК-3	знать основные направления и тенденции развития информаци сферы
	уметь находить, систематизировать ианализировать информацию различных источников
	владеть навыками эффективного применения программных сред используемых в современных поисковых системах
ПК-7	знать основные принципы построения защищенных распредел компьютерных систем
	уметь анализировать защищенность компьютерных систем
	владеть навыками выявления и устранения уязвимостей компьн систем
ПК-16	знать основные принципы построения систем обнаружения компьютерных атак
	уметь формализовать задачу управления безопасностью информационных систем
	владеть навыками проведения анализа рисков и администрир безопасности распределенных компьютерных систем

ПК-20	знать способы обнаружения и нейтрализации последствий вто в компьютерные системы
	уметь администрировать системы обнаружения компьютерных
	владеть навыками организации защищенного удаленного досту информационным ресурсам и способами настройки стандартны систем обнаружения компьютерных атак
ПСК-3.3	знатьнаправления и тенденции развития безопасных информац технологий
	уметь оценивать применимость информационных технологий для конкретных компьютерных систем
	владеть навыками адаптации новых программных средств к требованиям информационной безопасности
ПСК-3.4	знать формы и методы организационной деятельности в сфере защиты распределенных компьютерных систем
	уметь организовывать мероприятия по защите информ распределенных компьютерных системах
	владеть навыками применения организационных механизмо процессе защитеы информации в распределенных компьютерн системах

7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв7,8семестредляочной

«зачтено»

«незачтено»

Компе-тенция	Результатыобучения,характеризующие сформированностькомпетенции
ОПК-3	знать основные направления и тенденции развития информаци сферы
	уметь находить, систематизировать ианализировать информацию различных источников
	владеть навыками эффективного применения программных сред используемых в современных поисковых системах
ПК-7	знать основные принципы построения защищенных распредел компьютерных систем
	уметь анализировать защищенность компьютерных систем
	владеть навыками выявления и устранения уязвимостей компьн систем
ПК-16	знать основные принципы построения систем обнаружения компьютерных атак
	уметь формализовать задачу управления безопасностью информационных систем
	владеть навыками проведения анализа рисков и администрир безопасности распределенных компьютерных систем
ПК-20	знать способы обнаружения и нейтрализации последствий вто в компьютерные системы
	уметь администрировать системы обнаружения компьютерных
	владеть навыками организации защищенного удаленного досту информационным ресурсам и способами настройки стандартны систем обнаружения компьютерных атак
ПСК-3.3	знатьнаправления и тенденции развития безопасных информац технологий
	уметь оценивать применимость информационных технологий для конкретных компьютерных систем
	владеть навыками адаптации новых программных средств к требованиям информационной безопасности
ПСК-3.4	знать формы и методы организационной деятельности в сфере защиты распределенных компьютерных систем
	уметь организовывать мероприятия по защите информ распределенных компьютерных системах

	владеть навыками применения организационных механизмов процессе защитеы информации в распределенных компьютерны системах

или
«отлично»;
«хорошо»;
«удовлетворительно»;
«неудовлетворительно».

Компе- тенция	Результатыобучения,характеризующие сформированностькомпетенции	
ОПК-3	знать основные направления и тенденции развития информационной сферы	Тест
	уметь находить, систематизировать ианализировать информацию из различных источников	Решение ста
	владеть навыками эффективного применения программных средств, используемых в современных поисковых системах	Решение при предметной
ПК-7	знать основные принципы построения защищенных распределенных компьютерных систем	Тест
	уметь анализировать защищенность компьютерных систем	Решение ста
	владеть навыками выявления и устранения уязвимостей компьютерных систем	Решение при предметной
ПК-16	знать основные принципы построения систем обнаружения компьютерных атак	Тест
	уметь формализовать задачу управления безопасностью информационных систем	Решение ста
	владеть навыками проведения анализа рисков и администрирования безопасности распределенных компьютерных систем	Решение при предметной
ПК-20	знать способы обнаружения и нейтрализации последствий вторжений в компьютерные системы	Тест
	уметь администрировать системы обнаружения компьютерных атак	Решение ста
	владеть навыками организации защищенного удаленного доступа к информационным ресурсам и способами настройки стандартных систем обнаружения компьютерных атак	Решение при предметной
ПСК-3.3	знатьнаправления и тенденции развития безопасных информационных технологий	Тест
	уметь оценивать применимость информационных технологий для конкретных компьютерных систем	Решение ста
	владеть навыками адаптации новых программных средств к требованиям информационной безопасности	Решение при предметной
ПСК-3.4	знать формы и методы организационной деятельности в сфере защиты распределенных компьютерных систем	Тест
	уметь организовывать мероприятия по защите информации в распределенных компьютерных системах	Решение ста
	владеть навыками применения организационных механизмов в процессе защитеы информации в распределенных компьютерных системах	Решение при предметной

7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданияил

7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

1. Компьютерная атака - это:

а) реализация угрозы безопасности;

б) целенаправленное воздействие на компьютерную систему программно-технич

в) проявление уязвимости компьютерной системы.

2. Угрозы безопасности компьютерным системам могут быть классифицирован

а) по направленности реализации

б) по типу уязвимости;

в) по способу устранения негативных последствий.

3. Завершающим этапом компьютерной атаки является:

а) получение несанкционированного доступа;

б) маскировка следов атаки;

в) планирование атаки

4. Уязвимость компьютерной системы- это:

а) свойство ее компонента или процесса, путем использования которого может б

б) проявление воздействия угрозы безопасности;

в) нарушение работы средств защиты информации.

5. К идентификационным признакам контроля доступа к компьютерным системам отн

а) биометрические характеристики;

б) паспортные жанные;

в) IP-адрес компьютера.

7. К основнымнаправлениям контроля эффективности ЗИ в КС относятся:

а) мониторинг работы пользователей;

б) моделирование компьютерных атак;

в) проверка журналов системных событий.

8. В состав функций средств обнаружения вторжений входит:

а) конфигурирование сетевых устройств;

б) контроль работы системного администратора;

в) выявление атак и подозрительной сетевой активности.

9. Сеть-приманка - это:

а) защищенный ресурс, который служит объектом атак;

б) атакуемый фрагмент корпоративно сети;

в) средство выявления утечек информации.

10. Корпоративный центр ГосСОПКА должен включать в себя:

а) удостоверяющий центр ЭЦП;

б) центр операций по обеспечению безопасности;

в) центр управления ключевой информацией.

7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач

1. К техническим характеристикам электронных замков относится:

а) быстродействие;

б) способ считывания информации;

в) компания-производитель.

2. Рекомендации по использованию программных СЗИ нужны для:

а) выбора оптимального состава СЗИ;

б) подготовки эксплуатационной документации;
в) организации работы службы информационной безопасности.
3. В архитектуру типовой комплексной СЗИ для локальных сетей входит:
а) рабочее место администратора;
б) подсистема шифрования трафика;
в) криптоядро.
4. В защищенной операционной системе базовые средства защиты располагаются в:
а) прикладных программах;
б) ядре;
в) системных службах.
5. Риск компьютерной атаки рассчитывается как:
а) сумма ущербов от реализованной атаки;
б) произведение вероятности реализации атаки и возможного ущерба ;
в) произведение рейтинга атаки и ее длительности.
6. DOS-атака нарушает:
а) конфиденциальность;
б) доступность;
в) своевременность.
7. Основное свойство компьютерного вируса:
а) уничтожение информации;
б) размножение;
в) скрытность.
8. Системы контроля пользователей применяются для:
а) выявления инсайдерских утечек информации;
б) мониторинга внешней сетевой активности;
в) подтверждения лояльности сотрудников.
9. Для обнаружения компьютерных атак используются:
а) наборы правил;
б) сигнатуры;
в) шаблоны и макросы.
10. В число отличий локальной и корпоративной сетей входит:
а) количество сетевых соединений;
б) вид сетевого протокола;
в) расположение линий связи относительно контролируемой зоны.

7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач

1. Настройка веб-браузера для обеспечения безопасной работы в Интернет вклю
а) установку дополнений;
б) отключение всплывающих окон;
в) блокировку загрузки файлов.
2. Описание примерного алгоритма обнаружения атаки типа "отказ в обслужива
а) формулировки задачи;
б) перечисления контролируемых портов;
в) поиска злоумышленника.
3. Разграничение доступа пользователей на основе дискреционного принципа ко
а) ролей;

б) меток безопасности;
в) набора правил.
4. Функции управления СЗИ "Secret Net" разделяютя для:
а) пользователей сети;
б) сотрудников ИТ-службы;
в) администраторов безопасности.
5. Основные настройки персонального межсетевого экрана для обеспечения безопасной
а) входящий трафик;
б) отображение графики на экране;
в) количество запускаемых приложений.
6. Типовая структура подсистемы безопасности операционной системы включае
а) средства аутентификации;
б) сетевые драйверы;
в) модуль ввода-вывода.
7. Защищенная СУБД отличается наличием:
а) подсистемы безопасности;
б) средств шифрования;
в) сетевых служб.
8. Средства моделирования атак используют:
а) алгоритмы известных атак;
б) перебор случайных воздействий;
в) многократное повторение базовых операций ввод-вывода.
9. К техническим характеристикам средств обнаружения и блокирования сетевых атак
а) время реагирования;
б) наличие функции отключения;
в) нагрузочная способность.
10. Набор функций AAA для беспроводных сетей включает:
а) авторизацию;
б) ассоциацию;
в) атрибутизацию.

7.2.4Примерныйпереченьвопросовдляподготовкикзачету

1. Классификация угроз безопасности компьютерным системам.
2. Системные принципы защиты информации в компьютерных системах.
3. Стратегические направления государственной политики России в сфере проти
4. Методика построения комплексной защиты компьютерных систем.
5. Информационные технологии, повышающие защищенность компьютерных систем.
6. Структура и функции ГосСОПКА.
7. Методика расследования компьютерных атак
8. Характеристика средств защиты целостности и бесперебойности функционирования
9. Методика организации защищенного электропитания компьютерных систем.
10. Методы и средства контроля эффективности защиты информации в компьютерны

7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач

1. Описать алгоритм проведения атаки, направленной на получение НСД к инфо
2. Предложить обоснованное решение для организации контроля доступа к ком
3. Сделать ориентировочный расчет рисков для системы электронной почты коммерчес

4. Построить схему включения источников бесперебойного электропитания для
5. Обосновать выбор средств контроля доступа в помещение серверной объекта критич
6. Проранжировать способы удаления информации с компьютерных носителей по степе
7. Дать обоснованные рекомендации по использованию средств обеспечения конфиденц
8. Построить схему включения межсетевых экранов в сетевой структуре с налич
9. Сформулировать правила разграничения доступа к ресурсам сервера организа
10. Определить состав и количество компонентов системы защиты корпоративн

7.2.6.Методикавыставленияоценкиприпроведениипромежуточнойаттестац

Зачетпроводитсяпотест-билетам,каждыйизкоторыхсодержит5вопросовизадачу.К
1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабралменее2бал
2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентнабралот2до4балло
3.Оценка«Хорошо»ставитсявслучае,еслистудентнабралот5до7баллов.
4.Оценка«Отлично»ставится,еслистудентнабралот8до10баллов.

7.2.7Паспортоценочныхматериалов

№п/п	Контролируемыеразделы(тем
1	Системный подход к обеспечению защиты от компьютерных ата
2	Средства выявления и локализации уязвимостей компь безопасности
3	Методы и средства обнаружения и отражения сетевых атак
4	Комплексные системы защиты от компьютерных атак

7.3.Методическиематериалы,определяющиепроцедурыоцениваниязнаний,у

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирова
заданийнабумажномносителе.Времятестирования30мин.Затемосуществляетсяпроверк

Решениестандартныхзадачосуществляется,либоприпомощикомпьютернойсисте
яоценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестац

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютернойсистем
оценка,согласнометодикивыставленияоценкиприпроведениипромежуточнойаттестаци

8.1Переченьучебнойлитературы,необходимойдляосвоениядисциплины

1. Лукацкий А.В. Обнаружение атак, 2003, Печат.
2. Стивен Норткатт и др. Обнаружение вторжений в сеть. Настольная книга специ
3. Мак-Клар С. Хакинг в Web: атаки и защита, 2003, Печат.
4. Шелухин О.И. и др. Обнаружение вторжений в компьютерные сети (сетевые

Шелухин, О.И.
Системы обнаружения вторжений в компьютерные сети [Электронный ресурс] : учебное пособие / А.В. Савелов; А.Н. Руднев; О.И. Шелухин. - Системы обнаружения вторжений в компьютерные сети ; 2022-04-04. - Москва : Московский технический университет связи и информатики, 2013. - 88 c. URL: http://www.iprbookshop.ru/63360.html

5. Остапенко А.Г. Теория сетевых войн, 2015, Эл.ресурс.
6. Остапенко А.Г. Сетевое противоборство социотехнических систем2015, Эл.ресурс.
7. Остапенко А.Г. и др. Эпидемии в телекоммуникационных сетях, 2018, Печат.
8. Чирилло Дж. Обнаружение хакерских атак. Для профессионалов, 2002, Печат.
9. Белоножкин В.И Автоматизированные защищенные системы: учеб. пособие,
10.Белоножкин В.И., Системы обнаружения компьютерных атак (учебное пособие), 20
11. Кулаков В.Г. и др. Моделирование информационных операций и атак в сфе
12. Шумский А.А, .Шелупанов А. А. Системный анализ в защите информации, 20
13. Локхарт Э. Антихакинг в сети, 2005, Печат.
14. Остапенко Г.А., Радько Н.М. и др. Модели обнаружения сетевых вторжений : у

8.2Переченьинформационныхтехнологий,используемыхприосуществлениобразо телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданн

–Электронный журнал "*Информационная безопасность*", http://www.itsec.ru
–Электронный ресурс "Безопасность информационных систем", http://infobez.com
–Портал "Центр информационной безопасности" http://www.bezpeka.com/ru
–Портал «Anti-Malware» https://www.anti-malware.ru
–операционные системыMicrosoft Windows, Linux;
–офисное ПО «Libre Office»
–СУБД «Линтер»;
– СПО «Secret Net»;
– СПО «Vipnet client»;
– антивируное ПО «Kaspersky free”.

9МАТЕРИАЛЬНО-

Аудитория с компьютерными рабочими местами, локальная сеть, презентацион

10.МЕ

Подисциплине«Системыобнаружениякомпьютерныхатак»читаютсялекции,пров
Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсянаиболеесу
Практическиезанятиянаправленынаприобретениепрактическихнавыковиспользо

Вид учебных занятий	
Лекция	Написание конспекта ле понятий с помощью энц самостоятельно не удаетс
Практическое занятие	Конспектирование реком выполнение расчетно-гра
Самостоятельная работа	Самостоятельная работа - работа с текстами: учеб - выполнение домашних - работа над темами для с - участие в работе студен - подготовка к промежуто
Подготовка к промежуточной аттестации	Готовиться к промежуто зачетом с оценкой три дн