**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
«Информационные операции и атаки в распределенных компьютерных системах»

**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 _____/А.Е. Дешина/

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

Руководитель ОПОП _____/ А.Г. Остапенко /

Воронеж 2017

## 1. ЦЕЛИ И ЗАДАЧИ ДИСЦИПЛИНЫ

### 1.1. Цели дисциплины

Теоретическая и практическая подготовка студентов по вопросам защиты информации от информационных операций и атак в распределенных компьютерных системах

### 1.2. Задачи освоения дисциплины

- Изучение способов и средств защиты РКС;
-Освоение методов и средств контроля эффективности защиты информации в РКС от информационных операций и атак

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Информационные операции и атаки в распределенных компьютерных системах» относится к дисциплинам вариативной части (дисциплина по выбору) блока Б1.

## 3. ПЕРЕЧЕНЬ ПЛАНИРУЕМЫХ РЕЗУЛЬТАТОВ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Процесс изучения дисциплины «Информационные операции и атаки в распределенных компьютерных системах» направлен на формирование следующих компетенций:

ПК-14 - способностью организовывать работы по выполнению режима защиты информации, в том числе ограниченного доступа

ПСК-3.2- способностью анализировать защиту информации в распределенных компьютерных системах, проводить мониторинг, аудит и контрольные проверки работоспособности и защищенности распределенных компьютерных систем

| Компетенция | Результаты обучения, характеризующие сформированность компетенции |
|---|---|
| ПК-14 | Знать принципы и особенности функционирования проблемно-ориентированных систем управления, принятия решений и оптимизации технических объектов; |
| | Уметь применять современные системы противодействия информационным операциям и атакам |
| | Владеть техническими и программными средствами защиты РКС от атак. |
| ПСК-3.2 | Знать системы мониторинга, аудита и проверки работоспособности и защищенности распределенных компьютерных систем |
| | Уметь проверять работоспособность и защищенность распределенных компьютерных систем |
| | Владеть навыками построения систем защиты в |

| | |
|---|---|
| | распределенных компьютерных системах |

## 4. ОБЪЕМ ДИСЦИПЛИНЫ

Общаятрудоемкостьдисциплины«Информационныеоперацииатакиврас пределенныхкомпьютерныхсистемах»составляет10з.е.

Распределениетрудоемкостидисциплиныповидамзанятий

**очнаяформаобучения**

| Видыучебнойработы | Всегочасов | Семестры | |
|---|---|---|---|
| | | 9 | 10 |
| **Аудиторныезанятия (всего)** | 144 | 36 | 108 |
| В томчисле: | | | |
| Лекции | 90 | 18 | 72 |
| Практическиезанятия (ПЗ) | 54 | 18 | 36 |
| **Самостоятельнаяработа** | 180 | 54 | 126 |
| **Курсовойпроект** | + | | + |
| Часынаконтроль | 36 | - | 36 |
| Виды промежуточной аттестации - экзамен, зачет | + | + | + |
| Общая трудоемкость:<br>академические часы<br>зач.ед. | <br>360<br>10 | <br>90<br>2.5 | <br>270<br>7.5 |

## 5.СОДЕРЖАНИЕДИСЦИПЛИНЫ(МОДУЛЯ)

### 5.1Содержаниеразделовдисциплиныиираспределениетрудоемкостипо видамзанятий

**очнаяформаобучения**

| № п/п | Наименованиетемы | Содержаниераздела | Лекц | Практ. раб. | СРС | Всего, час |
|---|---|---|---|---|---|---|
| 1 | Анализ защищенности и обнаружения атак | Концепция адаптивного управления безопасностью; Технология анализа защищенности; Архитектура управления средствами сетевой безопасности; Аудит и мониторинг безопасности | 6 | 6 | 18 | 30 |
| 2 | Атаки на транспортную инфраструктуру сети | TCP-атаки. Затопление SYN-пакетами. Подделка TCP-сегмента.ICMP-атаки. Перенаправление трафика. Атаки Smurf, ping. UDP-атаки, IP-атаки, Сканирование сетей и портов, атаки на DNS, | 6 | 6 | 18 | 30 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | безопасность маршрутизации на основе BGP, Защита BGP, распределение функций между протоколами IPSec, Транспортный и тоннельный режимы, Протокол AH, Протокол ESP, Базы данных SAD и SPD, VPN на основе шифрования | | | | |
| 3 | Безопасность сетевых служб | Уязвимости, связанные с нарушением защиты оперативной памяти, Внедрение вредоносных программ, Троянские программы, Сетевые черви, Компьютерные вирусы, Приватность и куки, Протокол HTTPS, Облачные сервисы как источники угрозы | 6 | 6 | 18 | 30 |
| | | **Итого за 9-ый семестр** | 18 | 18 | 54 | 90 |
| 4 | Информационно-кибернетические операции: анализ и противодействие в отношении сетевых компьютерных атак | Классификация сетевых угроз для информационно-телекоммуникационных систем. Атаки на основе подбора имени и пароля посредством перебора. Атаки на основе сканирования портов. Атаки на основе анализа сетевого трафика. Атаки на основе внедрения ложного доверенного объекта. Атакинаосновеотказа в обслуживании. Оценкарисковкибернетическихатак | 24 | 12 | 42 | 78 |
| 5 | Безопасность протоколов маршрутизации | Протокол RIP:построение таблицы маршрутизации, адаптация к изменениям состояния сети, методы борьбы с ложными маршрутами; Протокол OSPF: метрики, построение таблиц маршрутизации; Протокол IGMP; Поддержка QoS: система интегрированного и дифференцированного обслуживания | 24 | 12 | 42 | 78 |

| | | | | | | |
|---|---|---|---|---|---|---|
| 6 | Технологии защиты межсетевого обмена данными в РКС | Проблемы обеспечения безопасности ОС; Технологии межсетевых экранов; Защита на канальном и сеансовом уровнях; Протокол PTPP; ПротоколL2TP; ПротоколSSL\TLS; ПротоколSOCKS; Инфраструктура защиты на прикладном уровне; Инфраструктура управления открытыми ключами PKI | 24 | 12 | 42 | 78 |
| | | **Итого за 10-ый семестр** | 72 | 36 | 126 | 234 |
| | | **Итого** | **90** | **54** | **180** | **324** |

**5.2Переченьлабораторныхработ**

Лабораторные работы не предусмотрены

## 6.ПРИМЕРНАЯТЕМАТИКАКУРСОВЫХПРОЕКТОВ(РАБОТ) ИКОНТРОЛЬНЫХРАБОТ

Всоответствиисучебнымпланомосвоениедисциплиныпредусматриваетвыполнениекурсовыхпроектовв10семестрахдляочнойформыобучения.

Примернаятематикакурсовогопроекта:«Проектирование защищенных РКС с использование аппаратно-программных систем»(по вариантам)

Курсовойпроектвключатвсебяграфическуючастьирасчетно-пояснительнуюзаписку.

## 7.ОЦЕНОЧНЫЕМАТЕРИАЛЫДЛЯПРОВЕДЕНИЯПРОМЕЖУТОЧНОЙАТТЕСТАЦИИОБУЧАЮЩИХСЯПОДИСЦИПЛИНЕ

### 7.1.Описаниепоказателейикритериевоцениваниякомпетенцийнаразличныхэтапахихформирования,описаниешкалоценивания

#### 7.1.1Этаптекущегоконтроля

Результатытекущегоконтролязнанийимежсессионнойаттестацииоцениваютсяпоследующейсистеме:

«аттестован»;

«неаттестован».

| Компе-тенция | Результатыобучения,характеризующие сформированностькомпетенции | Критерии оценивания | Аттестован | Неаттестован |
|---|---|---|---|---|
| ПК-14 | Знать принципы и особенности функционирования проблемно-ориентированных систем управления, принятия решений и оптимизации технических объектов; | Знание принципов и особенностей функционирования проблемно-ориентированных систем управления, принятия решений и оптимизации технических объектов; | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| | Уметь применять современные системы противодействия информационным | Умение применять современные системы противодействия информационным | Выполнение работ в срок, предусмотренный в рабочих | Невыполнение работ в срок, предусмотренный в рабочих |

| | | | | |
|---|---|---|---|---|
| | операциям и атакам | операциям и атакам | программах | программах |
| | Владеть техническими и программными средствами защиты РКС от атак. | Владение техническими и программными средствами защиты РКС от атак. | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| ПСК-3.2 | Знать системы мониторинга, аудита и проверки работоспособности и защищенности распределенных компьютерных систем | Знание систем мониторинга, аудита и проверки работоспособности и защищенности распределенных компьютерных систем | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| | Уметь проверять работоспособность и защищенность распределенных компьютерных систем | Умение проверять работоспособность и защищенность распределенных компьютерных систем | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |
| | Владеть навыками построения систем защиты в распределенных компьютерных системах | Владение навыками построения систем защиты в распределенных компьютерных системах | Выполнение работ в срок, предусмотренный в рабочих программах | Невыполнение работ в срок, предусмотренный в рабочих программах |

### 7.1.2Этаппромежуточногоконтролязнаний

Результатыпромежуточногоконтролязнанийоцениваютсяв9,10семестре дляочнойформыобученияподвух/четырехбалльнойсистеме:

«зачтено»
«незачтено»

| Компе-тенция | Результатыобучения,характеризующие сформированностькомпетенции | Критерии оценивания | Зачтено | Незачтено |
|---|---|---|---|---|
| ПК-14 | Знать принципы и особенности функционирования проблемно-ориентированных систем управления, принятия решений и оптимизации технических объектов; | Тест | Выполнениетеста на 70-100% | Выполнениеменее 70% |
| | Уметь применять современные системы противодействия информационным операциям и атакам | Решениестандартныхпрактическихзадач | Продемонстрирова н верный ход решения в большинстве задач | Задачинерешены |
| | Владеть техническими и программными средствами защиты РКС от атак. | Решение прикладных задач в конкретной предметной области | Продемонстрирован верный ход решения в большинстве задач | Задачинерешены |
| ПСК-3.2 | Знать системы мониторинга, аудита и проверки работоспособности и защищенности распределенных | Тест | Выполнениетеста на 70-100% | Выполнениеменее 70% |
| | Уметь проверять работоспособность и защищенность распределенных компьютерных систем | Решениестандартныхпрактическихзадач | Продемонстрирова н верный ход решения в большинстве задач | Задачинерешены |
| | Владеть навыками построения систем защиты в распределенных компьютерных системах | Решение прикладных задач в конкретной предметной области | Продемонстрирован верный ход решения в большинстве задач | Задачинерешены |

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

| Компе-тенция | Результатыобучения,характеризующие сформированностькомпетенции | Критерии оценивания | Отлично | Хорошо | Удовл. | Неудовл. |
|---|---|---|---|---|---|---|
| ПК-14 | Знать принципы и особенности функционирования проблемно-ориентированных систем управления, принятия решений и оптимизации технических объектов; | Тест | Выполнение тестана 90-100% | Выполнениетестана 80- 90% | Выполнениетестана 70- 80% | В тесте менее 70% правильных ответов |
| | Уметь применять современные системы противодействия информационным операциям и атакам | Решениестандартныхпрактическихзадач | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачинерешены |
| | Владеть техническими и программными средствами защиты РКС от атак. | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачинерешены |
| ПСК-3.2 | Знать системы мониторинга, аудита и проверки работоспособности и защищенности распределенных | Тест | Выполнение тестана 90-100% | Выполнениетестана 80- 90% | Выполнениетестана 70- 80% | В тесте менее 70% правильных ответов |
| | Уметь проверять работоспособность и защищенность распределенных компьютерных систем | Решениестандартныхпрактическихзадач | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачинерешены |
| | Владеть навыками построения систем защиты в распределенных компьютерных системах | Решение прикладных задач в конкретной предметной области | Задачи решены в полном объеме и получены верные ответы | Продемонстрирован верный ход решения всех, но не получен верный ответ во всех задачах | Продемонстрирован верный ход решения в большинстве задач | Задачинерешены |

## 7.2Примерныйпереченьоценочныхсредств(типовыеконтрольныезаданияилииныематериалы,необходимыедляоценкизнаний,умений,навыковви(или)опытадеятельности)

### 7.2.1Примерныйпереченьзаданийдляподготовкиктестированию

. Какое ведомство вырабатывает нормативно-правовые акты по защите коммерческой тайны?

а) МВД
б) ФСБ
в) СВР
г) ФСТЭК

2. Что не требуется реализовывать в подсистеме регистрации и учета ИТКС?

а) Учёт носителей информации
б) Обнуление освобождаемых областей оперативной памяти и внешних накопителей
в) Контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа
г) Сигнализация попыток нарушения защиты

3. Какие межсетевые экранов способны производить аутентификацию пользователя?

а) управляемые коммутаторы
б) шлюзы уровня приложений
в) шлюзы сеансового уровня
г) фильтрующие маршрутизаторы

4. Что относится к защите целостности на аппаратном уровне системы мер защиты информации?

а) использование маршрутизаторов и брандмауэров
б) применение технических средств аутентификации
в) специализация серверов
г) средства физической защиты технических средств

5. На каком уровне работает протокол IPSec?

а) на транспортном
б) на сетевом
в) на канальном
г) на сеансовом

6. Для какого вида деятельности применение тонких клиентов затруднительно?

а) банковская деятельность
б) обработка трехмерной графики
в) учебный процесс
г) оказание государственных и муниципальных услуг

7. Какая из приведенных мер защиты уменьшает вероятность достижения злоумышленником целей посредством реализации атаки типа «сканирование портов»?

а) Система идентификации и аутентификации
б) Криптографические средства

в) Системы обнаружения вторжений
г) Конфигурация системы

8. Какой из протоколов используется для аутентификации и безопасной передачи данных в сети Интернет?
а) IPSec
б) SSH
в) L2TP
г) TLS

9. Достоинством какого типа реализации VPN является легкость конфигурации и обслуживания в удаленных офисах?
а) VPN для брандмауэров
б) VPN на базе аппаратных средств
в) VPN на базе автономного программного обеспечения
г) VPN на базе маршрутизатора или коммутатора

10. Какой протокол подвержен атаке внедрения ложного объекта на основе использования недостатков алгоритмов удаленного поиска?
а) ICMP
б) UDP
в) ARP
г) TCP

**7.2.2Примерныйпереченьзаданийдлярешениястандартныхзадач**

1. Что понимается под системой, по которой информация может передаваться на расстоянии по линиям связи с применением цифровых технологий?
а) телекоммуникационная система
б) информационно-телекоммуникационная система
в) информационная система
г) коммуникационная система

2. Реализация какой удаленной атаки состоит в несанкционированном использовании протоколов управления сетью для изменения исходных таблиц маршрутизации?
а) Сетевой анализ
б) Подмена доверенного объекта
в) Внедрение ложного объекта на основе навязывания ложного маршрута
г) Внедрение ложного объекта на основе использования недостатков алгоритмов удаленного поиска

3. Что понимается под процедурой, в ходе которой проводится проверка подлинности отправителя или получателя сообщения
а) авторизация
б) аутентификация
в) верификация
г) аудит

4. Чем является совокупность условий и факторов, создающих потенциальную опасность, связанную с утечкой информации и/или несанкционированными и/или непреднамеренными воздействиями на нее?
а) уязвимость ИТКС

б) угроза ИТКС
в) уязвимость ИБ
г) угроза ИБ

5. Какой метод проверки пользователя преимущественно используется в корпоративных беспроводных сетях?
а) биометрический
б) аппаратный
в) непрямой
г) парольный

6. Что является основной целью практически любой атаки?
а) НСД к информации
б) искажение информации
в) уничтожение информации
г) разглашение перехваченной информации

7. От чего зависит коэффициент сложности процесса реализации атаки, характеризующий уровень необходимых навыков и оборудования для реализации атаки внутреннему злоумышленнику?
а) от уровня информатизации общества
б) от уровня компьютерной преступности общества
в) от вида системы
г) от масштаба организации

8. Каким из приведенных свойств обладает простейший поток?
а) свойством изменчивости
б) свойством стационарности
в) свойством последействия
г) свойством неординарности

9. К нарушению какого свойства защищенности информации приводит атака типа «сниффинг пакетов»
а) целостность
б) аутентичность
в) конфиденциальность
г) сохранность

10. Какой из способов реализации угроз проникновения в операционную систему компьютера подразумевает проверку наличия привилегий для отладки приложений?
а) незаконный захват привилегий
б) социальный инжиниринг
в) внедрение закладок
г) воздействие на систему аутентификации

### 7.2.3Примерныйпереченьзаданийдлярешенияприкладныхзадач

*(минимум10вопросовдлятестированиясвариантамиответов)*

### 7.2.4Примерныйпереченьвопросовдляподготовкикзачету

1. Концепция адаптивного управления безопасностью;ё
2. Технология анализа защищенности;
3. Архитектура управления средствами сетевой безопасности;
4. Аудит и мониторинг безопасности;

5. TCP-атаки. Затопление SYN-пакетами.
6. Подделка TCP-сегмента.ICMP-атаки.
7. Перенаправление трафика.
8. Атаки Smurf, ping.
9. UDP-атаки,
10. IP-атаки,
11. Сканирование сетей и портов, атаки на DNS,
12. Безопасность маршрутизации на основе BGP, Защита BGP,
13. Распределение функций между протоколами IPSec,
14. Транспортный и тоннельный режимы,
15. Протокол AH,
16. Протокол ESP,
17. Базы данных SAD и SPD,
18. VPN на основе шифрования,
19. Уязвимости, связанные с нарушением защиты оперативной памяти,
20. Внедрение вредоносных программ,
21.Троянские программы,
22. Сетевые черви,
23. Компьютерные вирусы,
24. Приватность и куки,
25. Протокол HTTPS,
26. Облачные сервисы как источники угрозы

### 7.2.5Примерныйпереченьзаданийдлярешенияприкладныхзадач

1.Классификация сетевых угроз для информационно-телекоммуникационных систем. 2.Атаки на основе подбора имени и пароля посредством перебора.

3. Атаки на основе сканирования портов.

4.Атаки на основе анализа сетевого трафика.

5. Атаки на основе внедрения ложного доверенного объекта.

6. Атаки на основе отказа в обслуживании.

7. Оценка рисков кибернетических атак;

8. Протокол RIP: построение таблицы маршрутизации, адаптация к изменениям состояния сети, методы борьбы с ложными маршрутами;

9.Протокол OSPF: метрики, построение таблиц маршрутизации;

10. Протокол IGMP; Поддержка QoS: система интегрированного и дифференцированного обслуживания;

11. Проблемы обеспечения безопасности ОС;

12. Технологии межсетевых экранов;

13. Защита на канальном и сеансовом уровнях;

14. Протокол PTPP;

15. Протокол L2TP;

16. Протокол SSL\TLS;

17. Протокол SOCKS;

18. Инфраструктура защиты на прикладном уровне;

19. Инфраструктура управления открытыми ключами PKI

### 7.2.6.Методикавыставлениояценкиприпроведениипромежуточной аттестации

*(Экзамен и зачет проводитсяпотест-билетам,каждыйизкоторыхсодержит10вопросовизадачу.Каждыйправильныйответнавопросвтестеоценивается1баллом,задачаоценивается в10баллов(5балловверноерешениеи5балловзаверныйответ).Максимал*

*ьноеколичествонабранныхбаллов–20.*

*1.Оценка«Неудовлетворительно»ставитсявслучае,еслистудентнабралменее6баллов.*

*2.Оценка«Удовлетворительно»ставитсявслучае,еслистудентнабралот6до10баллов*

*3.Оценка«Хорошо»ставитсявслучае,еслистудентнабралот11до15баллов.*

*4.Оценка«Отлично»ставится,еслистудентнабралот16до20баллов.)*

**7.2.7Паспортоценочныхматериалов**

| №п/п | Контролируемыеразделы(темы)дисциплины | Кодконтролируемойкомпетенции | Наименованиеоценочногосредства |
|---|---|---|---|
| 1 | Анализ защищенности и обнаружения атак | ПК-14 | Тест, контрольная работа, защита лабораторных работ, защита реферата |
| 2 | Атаки на транспортную инфраструктуру сети | ПК-14 | Тест, контрольная работа, защита лабораторных работ, защита реферата |
| 3 | Безопасность сетевых служб | ПК-14 | Тест, контрольная работа, защита лабораторных работ, защита реферата |
| 4 | Информационно-кибернетические операции: анализ и противодействие в отношении сетевых компьютерных атак | ПК-14 | Тест, контрольная работа, защита лабораторных работ, защита реферата |
| 5 | Безопасность протоколов маршрутизации | ПК-14 | Тест, контрольная работа, защита лабораторных работ, защита реферата, |
| 6 | Технологии защиты межсетевого обмена данными в РКС | ПК-14 | Тест, контрольная работа, защита лабораторных работ, защита реферата, |

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

Тестированиеосуществляется,либоприпомощикомпьютернойсистемытестирования,либосиспользованиемвыданныхтест-заданийнабумажномносителе.Времятестирования30мин.Затемосуществляетсяпроверкатестаэкзаменаторомивыставляетсяоценкасогласнометодикивыставлениояценкиприпроведении промежуточнойаттестации.

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

Решениеприкладныхзадачосуществляется,либоприпомощикомпьютерн ойсистемытестирования,либосиспользованиемвыданныхзадачнабумажномно сителе.Времярешениязадач30мин.Затемосуществляетсяпроверкарешениязада чэкзаменаторомивыставляетсяоценка,согласнометодикивыставлениояценкип рипроведениипромежуточнойаттестации.

Защитакурсовойработы,курсовогопроектаилиотчетаповсемвидампракт икосуществляетсясогласнотребованиям,предъявляемымкработе,описаннымв методическихматериалах.Примерноевремязащитынаодногостудентасоставля ет20мин.

## 8УЧЕБНОМЕТОДИЧЕСКОЕИИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ)

### 8.1Переченьучебнойлитературы,необходимойдляосвоениядисципл ины

Основная литература:


1. Владимиров И.В. Технический контроль безопасности информационно-телекоммуникационных систем [Электронный ресурс]: Учеб. пособие / И. В. Владимиров, Е. А. Москалёва. - Электрон. текстовые, граф. дан. (586 кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2012. - 1 файл. - 30-00.
2. Деревянко В.Н. Безопасность сетей ЭВМ [Электронный ресурс]: Учеб. пособие / В. Н. Деревянко. - Электрон. текстовые, граф. дан. (7,31 Мб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2014. - 1 файл. - 30-00.
3. Эпидемии в телекоммуникационных сетях [Текст] / Остапенко Александр Григорьевич [и др.]; под ред. Д. А. Новикова. - Москва: Горячая линия - Телеком, 2014. - 282 с.: ил. - (Теория сетевых войн. № 1). - Библиогр.: с. 231-245 (244 назв.). - ISBN 978-5-9912-0682-2: 736-00.


Дополнительная литература:


1. Остапенко, А.Г. Обнаружение и нейтрализация вторжений в распределенных информационных системах [Электронный ресурс]: Учеб. пособие / А. Г. Остапенко, М. Н. Иванкин. - Электрон. текстовые, граф. дан. (366 Кб). - Воронеж: ФГБОУ ВПО "Воронежский государственный технический университет", 2013. - 1 файл. - 30-00.
2. Методические указания к самостоятельным работам по дисциплинам «Информационные операции и атаки в распределенных компьютерных системах», «Оценка эффективности противодействия ИОА в РКС», «Информационные операции и атаки в распределенных информационных системах» для студентов специальностей 090301 «Компьютерная безопасность», 090303

«Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: Е. С. Соколова, Д. Г. Плотников. - Электрон. текстовые, граф. дан. (451 Кб). - Воронеж: ФГБОУ ВПО "Воронежскийгосударственныйтехническийуниверситет", 2014. - 1 файл. - 00-00.

3. Методические указания к курсовому проектированию по дисциплине «Информационные операции и атаки в распределенных информационных системах» для студентов специальности 090303 «Информационная безопасность автоматизированных систем» очной формы обучения [Электронный ресурс] / Каф. систем информационной безопасности; Сост.: Е. С. Соколова, Д. Г. Плотников. - Электрон. текстовые, граф. дан. (475 Кб). - Воронеж : ФГБОУ ВПО "Воронежскийгосударственныйтехническийуниверситет", 2014. - 1 файл. - 00-00.

**8.2Переченьинформационныхтехнологий,используемыхприосуществленииобразовательногопроцессаподисциплине,включаяпереченьлицензионногопрограммногообеспечения,ресурсовинформационно-телекоммуникационнойсети«Интернет»,современныхпрофессиональныхбазданныхиинформационныхсправочныхсистем:**

http://att.nica.ru
http://www.edu.ru/
http://window.edu.ru/window/library
http://www.intuit.ru/catalog/
https://marsohod.org/howtostart/marsohod2
http://bibl.cchgeu.ru/MarcWeb2/ExtSearch.asp
https://cchgeu.ru/education/cafedras/kafsib/?docs
http://www.eios.vorstu.ru
http://e.lanbook.com/ (ЭБС Лань)
http://IPRbookshop.ru/ (ЭБСIPRbooks)

## 9МАТЕРИАЛЬНО-ТЕХНИЧЕСКАЯБАЗА,НЕОБХОДИМАЯДЛЯОСУЩЕСТВЛЕНИЯОБРАЗОВАТЕЛЬНОГОПРОЦЕССА

Специализированная лекционная аудитория, оснащенная оборудованием для лекционных демонстраций и проекционной аппаратурой

Дисплейный класс, оснащенный компьютерными программами для проведения лабораторного практикума.

## 10.МЕТОДИЧЕСКИЕУКАЗАНИЯДЛЯОБУЧАЮЩИХСЯПООСВОЕНИЮДИСЦИПЛИНЫ(МОДУЛЯ)

Подисциплине«Информационныеоперацииатакиврасределенныхкомпьютерныхсистемах»читаютсялекции,проводятсялабораторныеработы,выполняетсякурсовойпроект.

Основойизучениядисциплиныявляютсялекции,накоторыхизлагаютсяна иболеесущественныеитрудныевопросы,атакжевопросы,ненашедшиеотражени явучебнойлитературе.

Лабораторныеработывыполняютсяналабораторномоборудованиивсоот ветствиисметодиками,приведеннымивуказанияхквыполнениюработ.

Методикавыполнениякурсовогопроектаизложенавучебно-методическо мпособии.Выполнятьэтапыкурсовогопроектадолжнысвоевременноивустанов ленныесроки.

Контрольусвоенияматериаладисциплиныпроизводитсяпроверкойкурсо вогопроекта,защитойкурсовогопроекта.

| 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:<br>- работа с текстами: учебниками, справочниками, дополнительной литературой, а также проработка конспектов лекций;<br>- выполнение домашних заданий и расчетов;<br>- работа над темами для самостоятельного изучения;<br>- участие в работе студенческих научных конференций, олимпиад;<br>- 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, экзаменом три дня эффективнее всего использовать для повторения и систематизации материала. |