МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Российский государственный гуманитарный университет»
(ФГБОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
ФАКУЛЬТЕТ ИНФОРМАЦИОННЫХ СИСТЕМ И БЕЗОПАСНОСТИ

Кафедра комплексной защиты информации

ТЕХНОЛОГИИ ЗАЩИТЫ ИНФОРМАЦИИ В КОМПЬЮТЕРНЫХ СЕТЯХ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ
Направление подготовки 09.04.03 Прикладная информатика
Направленность подготовки
Управление данными и знаниями в компьютерных сетях
Уровень высшего образования: магистратура

Форма обучения очная, очно-заочная, заочная

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2023

Технологии защиты информации в компьютерных сетях
Рабочая программа дисциплины
Составитель(и):
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой КЗИ Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры
комплексной защиты информации
№ 8 от 23.03. 2023 г.

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – профессиональная подготовка магистрантов, необходимая для освоения методов и технологий защиты информации в компьютерных сетях
Задачи дисциплины:
дать знания:
– о методах и средствах защиты информации в компьютерных сетях;
– о технологии межсетевого экранирования;
– о методах и средствах построения виртуальных частных сетей;
– о методах и средствах аудита защищённости информационных систем.

1.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенция	Индикаторы компетенций	Результаты обучения
ПК-6 – способность формировать стратегию информатизации прикладных процессов и создания прикладных информационных систем в соответствии со стратегией развития предприятий	ПК-6.1 – Знает теоретические основы стратегического управления предприятием и информационными технологиями	Знать: технологии обнаружения компьютерных атак и их возможности; основные уязвимости и типовые атаки на современные компьютерные системы; возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности; методы защиты компьютерных сетей при автоматизации информационных процессов и информатизации предприятий и организаций
	ПК-6.2 – Умеет анализировать потребности предприятия в информатизации, планировать развитие ИТ по направлениям	Уметь: выполнять настройку защитных механизмов сетевых программно-аппаратных средств; настраивать политику безопасности средствами программно-аппаратных комплексов сетевой защиты информации; организовывать защиту сегментов компьютерной сети с использованием межсетевых экранов
	ПК-6.3 – Владеет навыками формирования стратегии информатизации предприятия в соответствии со стратегией развития	Владеть: навыками администрирования сетевых программно-аппаратных комплексов защиты информации; навыками администрирования систем обнаружения компьютерных атак;

		навыками администрирования систем виртуальных частных сетей организации
ПК-5 – способность использовать современные методы оценки качества, надёжности и информационной безопасности информационных систем в процессе их проектирования и эксплуатации	ПК-5.1 – Знает современные методы оценки качества, надёжности и информационной безопасности информационных систем в процессе проектирования и эксплуатации	Знать: классификацию и общую характеристику сетевых программно-аппаратных средств защиты информации; особенности реализации методов защиты информации современными программно-аппаратными средствами; основные принципы администрирования защищённых компьютерных систем.
	ПК-5.2 – Умеет применять современные методы оценки качества, надёжности и информационной безопасности информационных систем в процессе проектирования и эксплуатации	Уметь: применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищённых компьютерных сетей.
	ПК-5.3 – Владеет навыками применения современных методов оценки качества, надёжности и информационной безопасности информационных систем в процессе проектирования и эксплуатации прикладных ИС"	Владеть: методикой проведения аудита информационной безопасности.

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Технологии защиты информации в компьютерных сетях» относится к дисциплинам части, формируемой участниками образовательных отношений блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин: «Теория информационных процессов и систем», «Архитектура предприятий и информационных систем», «Информатика», «Теоретические основы компьютерной безопасности».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Методы семантического поиска и обработки информации в компьютерных сетях», «Облачные технологии», «Методология и технология проектирования информационных систем».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 3 з.е., 108 академических часов.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
2	Лекции	**14**
2	Практические работы	**16**
	Всего:	**30**

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет _78__ академических часов.

Структура дисциплины для очно-заочной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
4	Лекции	**12**
4	Практические работы	**12**
	Всего:	**24**

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет _84_ академических часа.

Структура дисциплины для заочной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
2	Лекции	**4**
3	Лекции	**4**
3	Практические работы	**4**
	Всего:	**12**

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет _96__ академических часа(ов).

3. Содержание дисциплины

Тема 1. Основные уязвимости и виды атак на компьютерные системы
Виды атак на компьютерные системы (КС). Основные уязвимости КС. Несанкционированный доступ к информации (НСД). Утечка информации. Виды защиты от НСД и утечки информации. Организационно-правовые методы защиты информации. Классификация автоматизированных систем и средств вычислительной техники по уровню защите от НСД.

Тема 2. Защита информации в компьютерных сетях
Основы сетевых технологий. Топология сетей. Модель ISO/OSI и TCP/IP. Маршрутизация. Основные сетевые устройства.
Разграничение доступа к защищаемым ресурсам. Модели доступа к защищаемым ресурсам**.** Методы аутентификации. Парольная защита, способы организации, достоинства и недостатки. Виды средств и систем защиты информации. Межсетевое экранирование. Принципы межсетевого экранирования. Демилитаризованная зона. Классификация межсетевых экранов. Виртуальные частные сети. Принципы их работы. Электронно-цифровая подпись. Защищённый электронный документооборот в организации. Администрирование встроенных и добавочных систем защиты информации. Операционные системы MS Windows и MS Windows Server. Комплексная система защиты информации «Панцирь-К».

Тема 3. Средства обнаружения компьютерных атак и аудит безопасности компьютерных систем
Средства обнаружения компьютерных атак, их назначение, принципы работы. Средства предотвращения компьютерных атак. Аудит безопасности сетей, его виды и цели. Основные этапы аудита безопасности. Средства сетевого аудита. Отчёт об аудите сетевой безопасности.

4. Образовательные технологии

Для проведения учебных занятий по дисциплине используются различные образовательные технологии. Для организации учебного процесса может быть использовано электронное обучение и (или) дистанционные образовательные технологии.

5. Оценка планируемых результатов обучения

5.1. Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *- опрос (темы 1-3)* *- практические работы № 1-3*	 *10 баллов* *10 баллов*	 *30 баллов* *30 баллов*
Промежуточная аттестация *Экзамен*		*40 баллов*
Итого за семестр *Экзамен*		*100 баллов*

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A, B	«отлично» / «зачтено (отлично)» / «зачтено»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо» / «зачтено (хорошо)» / «зачтено»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D, E	«удовлетворительно» / «зачтено (удовлетворительно)» / «зачтено»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной атте-

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		стации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F, FX	«неудовлетворительно» / не зачтено	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3. Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний обучающегося по определённому разделу, теме, проблеме и т.п.

.

Перечень устных вопросов для проверки знаний

1. Виды атак на компьютерные системы.
2. Классификация уязвимостей компьютерных систем.
3. Модели защиты от НСД.
4. Топологии сетей.
5. Модель ISO/OSI.
6. Устройства первого уровня модели ISO/OSI.
7. Устройства второго уровня модели ISO/OSI.
8. Устройства третьего уровня модели ISO/OSI.
9. Парольная защита, способы организации, достоинства и недостатки..
10. Методы аутентификации.
11. Межсетевое экранирование
12. Демилитаризованная зона.
13. Виртуальные частные сети. Принципы их работы
14. Администрирование встроенных и добавочных систем защиты информации
15. Средства обнаружения и предотвращения компьютерных атак
16. Виды и цели аудита безопасности сетей.
17. Основные этапы аудита безопасности?

Примерные задания для тестирования

1. Уязвимость – это:

а) *любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы*

б) любая обнаруженная характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы

в) любая выявленная характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы

2. Укажите, на каких этапах жизненного цикла системы возможно возникновения уязвимостей:

а) на этапе проектирования

б) на этапе реализации

в) на этапе эксплуатации

г) *на всех трёх перечисленных этапах*

Примерные вопросы к зачёту с оценкой

1. Классификация атак на компьютерные системы.
2. Основные уязвимости компьютерных систем.
3. Виды несанкционированного доступа к информации.
4. Понятие утечки информации. Основные каналы утечки.
5. Виды защиты от НСД и утечки информации.
6. Организационно-правовые методы защиты информации.
7. Классификация автоматизированных систем и средств вычислительной техники по уровню защите от НСД.
8. Дискреционная модель доступа к защищаемым ресурсам.
9. Мандатная модель доступа к защищаемым ресурсам
10. Методы аутентификации.
11. Парольная защита, способы организации, достоинства и недостатки.
12. Виды средств и систем защиты информации.
13. Принципы межсетевого экранирования.
14. Организация демилитаризованной зона.
15. Классификация и принципы межсетевых экранов.
16. Принципы построения и работы виртуальные частные сети.
17. Принципы работы электронно-цифровая подпись.
18. Организация защищённого электронного документооборота в компании.
19. Администрирование встроенных и добавочных систем защиты информации.
20. Администрирование встроенной системы защиты информации ОС семейства MS Windows (локально)
21. Администрирование встроенной системы защиты информации ОС семейства MS Windows Server.
22. Комплексная система защиты информации «Панцирь-К».
23. Средства обнаружения компьютерных атак, их назначение, принципы работы.
24. Средства предотвращения компьютерных атак.
25. Аудит безопасности сетей, его виды и цели.
26. Основные этапы аудита безопасности.
27. Средства сетевого аудита.
28. Структура отчёт об аудите сетевой безопасности

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

Основные

1. *Федеральный закон* от 27 июля 2006 г. №149-ФЗ «Об информации, информационных технологиях и о защите информации» (с изм. и доп., посл. от 01.05.2019). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
2. *Руководящий документ*. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g, свободный. – Загл. с экрана.
3. *Руководящий документ*. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2, свободный. – Загл. с экрана.
4. *Руководящий документ*. Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g, свободный. – Загл. с экрана.

Дополнительные

5. *Руководящий докумен*т. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3, свободный. – Загл. с экрана.
6. *Руководящий документ.* Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. N 114
7. *Федеральный закон* «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

Литература

Основная

1. *Щеглов, А. Ю.* Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – Москва : Издательство Юрайт, 2019. – 309 с. – (Бакалавр и магистр. Академический курс). – ISBN 978-5-534-04732-5. – Текст : электронный // ЭБС Юрайт [сайт]. – URL: https://www.biblio-online.ru/bcode/433715 (дата обращения: 23.08.2019).
2. *Шаньгин В.Ф.* Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. – Москва : ИД «ФОРУМ» : ИНФРА-М, 2019. – 592 с. – (Высшее образование: Бакалавриат). – Текст : электронный. – URL: https://new.znanium.com/catalog/product/996789
3. *Яновский Г.Г.* Сети связи: Учебник / Гольдштейн Б.С., Соколов Н.А., Яновский Г.Г. – СПб:БХВ-Петербург, 2014. – 401 с. – Режим доступа: http://znanium.com/catalog /product/944261
4. *Щеглов, А. Ю.* Защита информации: основы теории : учебник для бакалавриата и магистратуры / А. Ю. Щеглов, К. А. Щеглов. – Москва : Издательство Юрайт, 2019. – 309 с. – (Серия : Бакалавр и магистр. Академический курс). – ISBN 978-5-534-04732-5. — Текст : электронный // ЭБС Юрайт [сайт]. – URL: https://www.biblio-online.ru/book/zaschita-informacii-osnovy-teorii-433715

Дополнительная

5. *Помешкин, А. А.* Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса "Secret Net 5.0" / Помешкин А.А., Коротких И.В. - Новосибирск :НГТУ, 2012. - 47 с.: ISBN 978-5-7782-1990-8. - Текст : электронный. - URL: https://new.znanium.com/catalog/product/556699 (дата обращения: 23.08.2019).

6.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет».

1. ОХРАНА.ru. Российское СМИ о безопасности. [Электронный ресурс] : Режим доступа : https://oxpaha.ru/, свободный. – Загл. с экрана.
2. Sec.ru. Портал по безопасности. [Электронный ресурс] : Режим доступа : http://sec.ru/, необходима регистрация. – Загл. с экрана.
3. *Банк данных угроз безопасности информации*. [Электронный ресурс] / ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России» – Режим доступа : http://sec.ru/, свободный. – Загл. с экрана.
4. *НПП «Информационные технологии в бизнесе»*. [Электронный ресурс] : Режим доступа : http://www.npp-itb.ru/products/, свободный. – Загл. с экрана.
5. *Компания «Код Безопасности».* [Электронный ресурс] : Режим доступа : https://www.securitycode.ru/products/, свободный. – Загл. с экрана.

6.3. Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7. Материально-техническое обеспечение дисциплины

Для материально-технического обеспечения дисциплины необходимо:

1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должно быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2) для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное
4	Cisco Packet Tracer v.7.2 и выше	Cisco Systems	свободное

8. Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;

– обеспечивается индивидуальное равномерное освещение не менее 300 люкс;

– для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;

– письменные задания оформляются увеличенным шрифтом;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

– лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;

– письменные задания выполняются на компьютере в письменной форме;

– экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

– лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

– письменные задания выполняются на компьютере со специализированным программным обеспечением;

– экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

– в печатной форме увеличенным шрифтом;
– в форме электронного документа;
– в форме аудиофайла.

- для глухих и слабослышащих:

– в печатной форме;
– в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

– в печатной форме;
– в форме электронного документа;
– в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:

– устройством для сканирования и чтения с камерой SARA CE;
– дисплеем Брайля PAC Mate 20;
– принтером Брайля EmBraille ViewPlus;

- для глухих и слабослышащих:

– автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
– акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата:

– передвижными, регулируемыми эргономическими партами СИ-1;
– компьютерной техникой со специальным программным обеспечением.

9. Методические материалы

9.1. Планы практических занятий – проверка сформированности компетенций – ПК-5 и ПК-6

Тема 2 (6 ч.) Защита информации в компьютерных сетях

Задания:

1. Разработать систему защиты информации для фирмы (список и структура фирм предлагается преподавателем).
2. Провести анализ объектов информатизации и разработать систему разграничения доступа.
3. Работа с межсетевыми экранами. Создание демилитаризованной зоны.
4. Организация защищённого электронного документооборота.
5. Произвести изменения с учётом вводной: фирма получила контракт по Гособоронзаказу и получила право работать с информацией, имеющей гриф «секретно».

Указания по выполнению заданий:

1. Изучить теоритический материал по теме.

2. Изучить документацию на систему защиты информации «Панцирь-К» для администратора.
3. Ответить на теоритические вопросы в конце лабораторной работы

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной.
2. Система защиты информации «Панцирь-К» или аналог или эмулятор.
3. Система электронного документооборота

Тема 3 (4 ч.) Средства обнаружения компьютерных атак и аудит безопасности компьютерных систем

Задания:

1. Развернуть систему обнаружения вторжений.
2. Провести настройку системы обнаружения вторжений.
3. Спланировать аудит сетевой безопасности фирмы.
4. Провести детальный анализ информационных ресурсов.
5. Провести тесты на проникновение.

Указания по выполнению заданий:

1. Изучить теоритический материал по теме.
2. Ответить на теоритические вопросы в конце лабораторной работы

Список литературы:

Приведён в п. 6 данной РПД

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС MS Windows, виртуальной машиной программным обеспечением для тестирования и аудита.

По результатам практического занятия обучающиеся составляют отчёт, структура которого представлена ниже. Отчёт составляется в электронной форме с использованием MS Office 2007 и выше и передаётся преподавателю посредством оговорённой формы связи.

Приложение 1. Аннотация дисциплины

АННОТАЦИЯ ДИСЦИПЛИНЫ

Цель дисциплины: профессиональная подготовка магистрантов, необходимая для освоения методов и технологий защиты информации в компьютерных сетях.

Задачи: дать знания:

о методах и средствах защиты информации в компьютерных сетях;

о технологии межсетевого экранирования;

о методах и средствах построения виртуальных частных сетей;

о методах и средствах аудита защищённости информационных систем.

В результате освоения дисциплины обучающийся должен:

Знать:

технологии обнаружения компьютерных атак и их возможности; основные уязвимости и типовые атаки на современные компьютерные системы;

возможности и особенности использования специализированных программно-аппаратных средств при проведении аудита информационной безопасности;

методы защиты компьютерных сетей при автоматизации информационных процессов и информатизации предприятий и организаций

классификацию и общую характеристику сетевых программно-аппаратных средств защиты информации;

особенности реализации методов защиты информации современными программно-аппаратными средствами;

основные принципы администрирования защищённых компьютерных систем.

Уметь:

выполнять настройку защитных механизмов сетевых программно-аппаратных средств;

настраивать политику безопасности средствами программно-аппаратных комплексов сетевой защиты информации;

организовывать защиту сегментов компьютерной сети с использованием межсетевых экранов;

применять механизмы защиты, реализованные в программно-аппаратных комплексах, с целью построения защищённых компьютерных сетей.

Владеть:

навыками администрирования сетевых программно-аппаратных комплексов защиты информации;

методикой проведения аудита информационной безопасности.