ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

Утверждено:
на заседании кафедры
протокол № 8 от « 24 » февраля 2021 г.
Зав. кафедрой _____/А.С. Исмагилова

Согласовано:
Председатель УМК ИИГУ
_____/Р.А. Гильмутдинова

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информационных процессов в компьютерных сетях
базовая часть

программа специалитета

Направление
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Направленность подготовки
Технологии защиты информации в правоохранительной сфере

Квалификация
специалист

Разработчики (составитель) Ассистент	_____/А.Ф. Фатхелисламов

Для приема: 2021 г.
Уфа - 2021

Составитель / составители: А.Ф. Фатхелисламов

Рабочая программа дисциплины *утверждена* на заседании кафедры управления информационной безопасностью протокол от «_24_» февраля 2021 г. №_8

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры _____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры _____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры _____,
протокол № ____ от «____» _____ 20 _ г.

Заведующий кафедрой _____/ _____Ф.И.О/

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

По итогам освоения дисциплины обучающийся должен достичь следующих результатов обучения:

Категория (группа) компетенций[1] (при наличии ОПК)	**Формируемая компетенция (с указанием кода)**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения по дисциплине**
Системноеикритическоемышление	ПК-1 Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей	ПК-1.1 Знать основные требования по защите информации и политики безопасности компьютерных систем и сетей	Знает основные требования по защите информации и политики безопасности компьютерных систем и сетей
		ПК-1.2 Уметь применять основные требования по защите информации и политики безопасности компьютерных систем и сетей	Умеет применять основные требования по защите информации и политики безопасности компьютерных систем и сетей
		ПК-1.3 Владеть основными требования по защите информации и политики безопасности компьютерных систем и сетей	Владеет основными требования по защите информации и политики безопасности компьютерных систем и сетей

[1] Указывается только для УК и ОПК (при наличии).

2. Место дисциплины в структуре образовательной программы

Дисциплина «Защита информационных процессов в компьютерных сетях» относится к базовой части образовательной программы.

Дисциплина изучается на 4-ом курсе в 7, 8 семестре.

Эти дисциплины направлены на формирование компетенций ПК-1.

3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)

Содержание рабочей программы представлено в Приложении 1.

4. Фонд оценочных средств по дисциплине

4.1. Перечень компетенций ииндикаторов достижения компетенций с указанием соотнесенных с ними запланированных результатов обучения по дисциплине. Описание критериев и шкал оценивания результатов обучения по дисциплине.

ПК-1: Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: основные положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрическо	Не знает	В целом знает основные положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и	Знает основные понятия и задачи в области теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации	Демонстрирует целостность знания об основных понятиях и задачах в теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки

	й связи для решения профессиональных задач		кодирования, электрической связи для решения профессиональных задач	и кодирования, электрической связи для решения профессиональных задач	сигналов, информации и кодирования, электрической связи для решения профессиональных задач
Второй этап (уровень)	Уметь: применять основные положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения профессиональных задач	Не умеет	Умеет применять основные положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения поставленной задачи.	Уверенно применяет основные положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения поставленной задачи, но допускает незначительные ошибки.	Уверенно применяет основные положения теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов, информации и кодирования, электрической связи для решения поставленной задачи.
Третий этап (уровень)	Владеть: основными методами теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов,	Не владеет	Владеет основными методами теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов,	Владеет основными методами теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов,	Владеет основными методами теорий электрических цепей, радиотехнических сигналов, распространения радиоволн, цифровой обработки сигналов,

	информации и кодирования, электрической связи для решения профессиональных задач		информации и кодирования, электрической связи для решения профессиональных задач, но без учета основных требований информационной безопасности	информации и кодирования, электрической связи для решения профессиональных задач, но испытывает незначительные трудности при обеспечении информационной безопасности.	информации и кодирования, электрической связи для решения профессиональных задач с учетом основных требований информационной безопасности.

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей, перечисленных в рейтинг-плане дисциплины (для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкала оценивания для зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов).

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций.Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
ПК-1: Способность формировать и реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации, с	*Знать:*политики, стратегии и технологии информационной безопасности и защиты информации, способы их организации иоптимизации	Устный индивидуальный / групповой опрос, защита практической работы, тестирование, коллоквиум
	*Уметь:*использовать закономерности преобразования данных в каналах при выполнении комплекса мер по информационной	Устный индивидуальный / групповой опрос, защита практической работы, тестирование, коллоквиум

учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз	безопасности	
	Владеть: навыками формирования комплекса мер (правила, процедуры, практические приемы и пр.) для управления информационной безопасностью	Устный индивидуальный / групповой опрос, защита практической работы, тестирование, коллоквиум

Рейтинг – план дисциплины*(при необходимости)*

Защита информационных процессов в компьютерных сетях

(название дисциплины согласно рабочему учебному плану)

направление/специальность10.05.05 Безопасность информационных технологий в правоохранительной сфере

курс 4, семестр8

Виды учебной деятельности студентов	**Балл за конкретное задание**	**Число заданий за семестр**	**Баллы**	
			Минимальный	**Максимальный**
Модуль 1. Преобразование аналоговых сообщений в цифровую форму и эффективное представление цифровых сообщений				
Текущий контроль			**0**	**20**
1. Аудиторная работа (допуски к лабораторным работам)	4	3	0	12
2. Домашние задания (оформление лабораторных работ)	2,5	3	0	8
Рубежный контроль			**0**	**15**
1.Тесты	10	1	0	10
2. Устный опрос	5	1	0	5
Модуль 2. Каналы связи и их математические модели				
Текущий контроль			**0**	**20**
1. Аудиторная работа (допуски к лабораторным работам)	3	5	0	15
2. Домашние задания (оформление лабораторных работ)	1	5	0	5
Рубежный контроль			**0**	**15**
1.Устный опрос	15	1	0	15
Поощрительные баллы				
1. Студенческая олимпиада	5			5
2. Участие в конференциях	5			5
3. Публикация статей	5			5
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
Посещение лекционных занятий			0	–6

2. Посещение практических (семинарских, лабораторных занятий)			0	–10
Итоговый контроль				
Экзамен			0	30

Устный индивидуальный опрос

Устный индивидуальный опрос проводится после изучения новой темы с целью выяснения наиболее сложных вопросов, степени усвоения информации.

Студент излагает содержание вопроса изученной темы.

Критерии и методика оценивания:

- 5 баллов выставляется студенту, если точно используется специализированная терминология, показано уверенное владение нормативной базой;

- 4 балла выставляется студенту, допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется специализированная терминология;

- 3 балла выставляется студенту, нет общего понимания вопроса, имеются затруднения или допущены ошибки в определении понятий, использовании терминологии.

Устный групповой опрос

Устный групповой опрос проводится после изучения новой темы с целью выяснения наиболее сложных вопросов, степени усвоения информации, поддержания внимания слушающей аудитории.

Критерии и методика оценивания:

- 5 баллов выставляется студенту, если точно используется специализированная терминология, показано уверенное владение нормативной базой;

- 4 балла выставляется студенту, допущены один-два недочета при освещении основного содержания ответа, нет определенной логической последовательности, неточно используется специализированная терминология;

- 3 балла выставляется студенту, нет общего понимания вопроса, имеются затруднения или допущены ошибки в определении понятий, использовании терминологии.

Тестирование

1. В число универсальных сервисов безопасности входят:

1) шифрование

2) средства построения виртуальных частных сетей туннелирование

2. Комплексное экранирование может обеспечить:

1) разграничение доступа по сетевым адресам

2) выборочное выполнение команд прикладного протокола

контроль объема данных, переданных по TCP-соединению

3. Уровень безопасности С, согласно «Оранжевой книге», характеризуется:

1) произвольным управлением доступом

2) принудительным управлением доступом верифицируемой безопасностью

4. Перехват данных является угрозой:

1) доступности

2) конфиденциальности целостности

5. В число целей политики безопасности верхнего уровня входят:

1) формулировка административных решений по важнейшим аспектам реализации программы безопасности

2) выбор методов аутентификации пользователей обеспечение базы для соблюдения законов и правил

6. «Общие критерии» содержат следующие виды требований:

1) функциональные
2) доверия безопасности
3) экономической целесообразности

7. Совместно с криптографическими сервисами туннелирование может применяться для достижения следующих целей:

1) обеспечение гарантированной полосы пропускания
2) обеспечение высокой доступности сетевых сервисов
3) обеспечение конфиденциальности и целостности передаваемых данных

8. Укажите наиболее существенные с точки зрения безопасности особенности современных российских ИС:

1) доминирование платформы Wintel
2) наличие подключения к Internet
3) наличие разнородных сервисов

9. Уголовный кодекс РФ не предусматривает наказания за:

1) увлечение компьютерными играми в рабочее время
2) неправомерный доступ к компьютерной информации
3) нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети

10. Уголовный кодекс РФ не предусматривает наказания за:

1) неправомерный доступ к компьютерной информации
2) создание, использование и распространение вредоносных программ
3) массовую рассылку запрещённойрекламной информации

Творческое задание (презентация, доклад)

Выполняется по результатам изучения темы дисциплины с целью дополнения практического материала.

Примеры тем творческих заданий

1. Реализация подсистем защиты в операционных системах. Подсистема защиты операционных систем семейства WindowsNT. Подсистема защиты операционных систем семейства UNIX.
2. Типовые сценарии атак на операционные системы.
3. Использование разрушающих программных средств.
4. Классификация удаленных атак.
5. Атаки подмены одной из сторон взаимодействия.
6. Перехват данных по принципу man-in-the-middle.
7. Атаки отказа в обслуживании.
8. Прослушивание и анализ трафика анализаторами протоколов. Сбор информации об удаленном узле, удаленной сети. Технологии сканирования.
9. Атаки на сетевую инфраструктуру для подмены одной из взаимодействующих сторон.
10. Ложные ARP-ответы и DNS-ответы. Навязывание хосту ложного маршрута средствами ICMP. Подмена одной из сторон в соединении TCP.

Критерии и методика оценивания:

Подготовленная и оформленная в соответствии с требованиями работа (презентация, доклад) оценивается преподавателем по следующим критериям:

- уровень эрудированности автора по изученной теме (знание автором состояния изучаемой проблематики, цитирование источников, в т.ч. НПА);
- логичность подачи материала, грамотность автора;
- соответствие работы всем стандартным требованиям к оформлению;
- знания и умения на уровне требований стандарта данной дисциплины: знание фактического материала, усвоение общих понятий и идей.
- 0 баллов выставляется студенту, если работа не соответствует критериям;

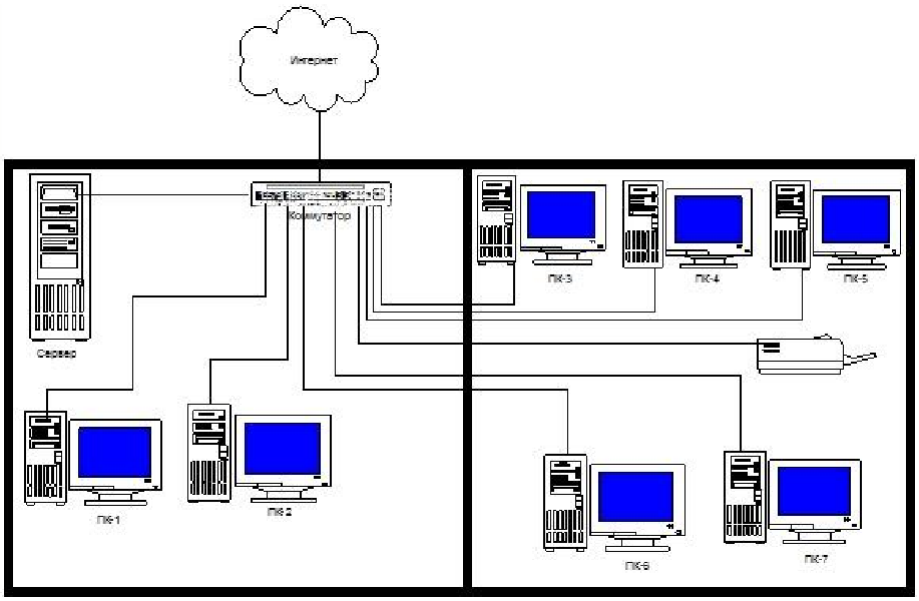
- 1 балл выставляется студенту, если работа частично соответствует критериям;
- 2 балла выставляется студенту, если работа соответствует критериям, но отсутствует логичность изложения информации;

– 3 балла выставляется студенту, если работа полностью соответствует критериям.

Контрольная работа

Содержание работы. Для локальной сети, согласно вашему варианту, разработать систему защиты информации.

1–й этап. Производится описание базовой системы;
2–й этап. Определяются уязвимости базовой системы;
3–й этап. Определяются угрозы для базовой системы;
4–й этап. Определяются нарушители базовой системы;
5–й этап. Определяется система защиты с набором барьеров;
6–й этап. Определяется возможные затраты при реализации различных угроз и их комбинаций – строится дерево сценариев.



Критерии и методика оценивания:

- 5 баллов выставляется студенту, если работа выполнена в полном объеме и изложена грамотным языком в определенной логической последовательности с точным использованием специализированной терминологии; показано уверенное владение нормативной базой;
- 4 балла выставляется студенту, если работа выполнена в полном объеме,

но имеет один из недостатков:

в работе допущены один-два недочета при освещении основного содержания ответа;

нет определенной логической последовательности, неточно используется специализированная терминология;

- 3 баллов выставляется студенту, если работа выполнена неполно, не показано общее понимание вопроса, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии, при знании теоретического материала выявлена недостаточная сформированность основных умений и навыков.

Типовые материалы к зачету

1. Атаки, основанные на ошибках в реализации сетевых служб.
2. Атаки распределенного отказа в обслуживании.
3. Трехуровневая и четырехуровневая модель.
4. Методики выявления и предотвращения атак отказа в обслуживании. Атаки отказа в обслуживании на NetBIOS/SMB.
5. Типы МЭ. Размещение межсетевых экранов.
6. Фильтры пакетов и необходимость фильтрации.
7. МЭ с двумя интерфейсами и тремя интерфейсами.
8. Построение и применение правил фильтрации. Списки доступа фильтров пакетов. Фильтры пакетов, ориентированные и неориентированные на соединения.
9. Трансляция сетевых адресов и портов.
10. NAT. Ограничения использования NAT. Механизм трансляции адресов и портов.

Критерии оценки (в баллах):

- «Зачтено» выставляется студенту, если он набрал по результатам изучения дисциплины 60 баллов;

- «Не зачтено» выставляется студенту, если он набрал менее 59 баллов.

Экзаменационные вопросы:

1. Классификация сетей. Сети, входящие в состав Единой сети электросвязи РФ.
2. Основные понятия в области связи: абонент, оператор связи, сеть связи, электросвязь, линейно-кабельные сооружения связи, линии связи и др.
3. Иерархические уровни в ТфОП: международная, междугородняя и т.д.
4. Городские телефонные сети.
5. Сельские телефонные сети.
6. Технологии коммутации.
7. Цифровизация ГТС.
8. Цифровизация СТС.
9. Системы сигнализации ТфОП.
10. Средства поддержки услуг ТфОП: ISDN, интеллектуальная сеть и др.
11. Основные понятия в области сотовой связи: мобильные и базовые станции, соты, хендовер. Стандарты в области СПС.
12. Технологии сотовой связи первого и второго поколений. Технология GSM.
13. Мобильная связь третьего поколения 3G. Технология UMTS.
14. Мобильная связь третьего поколения 4G. Технология LTE.
15. Услуги, поддерживаемые СПС.
16. Основные характеристики Bluetooth-соединения. Стандарты Bluetooth.
17. Методы разделения каналов в радиосвязи: временное (TDMA), частотное (FDMA), кодовое (CDMA). Их применение.
18. Методы расширения спектра DSSS и OFDM.
19. Метод расширения спектра FHSS, его использование в системах CDMA.
20. Пикосеть. Устройства Bluetooth.
21. СтандартыIEEE 802.11: IEEE 802.11, IEEE 802.11a, IEEE 802.11b, IEEE 802.11ac.
22. Стандарты IEEE 802.11: IEEE 802.11g, IEEE 802.11n, IEEE 802.11s.

23. Режимы работы Wi-Fi.
24. Устройства Wi-Fi. Технология WDS.
25. Беспроводные сетевые технологии. Планирование и развертывание сети Wi-Fi.
26. Технология VoIP. Архитектура SIP.
27. Технология VoIP. Архитектура сети H.323.
28. Обработка речевого сигнала при его передаче в сети VoIP.
29. Адресация в SIP.
30. Сообщения SIP.
31. Протоколы стека TCP/IP.
32. Цифровые и аналоговые сигналы. Модулирование и кодирование сигналов.
33. Стандартизация в связи.
34. Фундаментальные закономерности в области связи: теорема Котельникова и др.
35. Сетевые технологии.
36. Топологии компьютерных сетей.
37. Уровни OSI.
38. Протоколы прикладного и транспортного уровней OSI.
39. Протоколы канального и сетевого уровней OSI.
40. Основные устройства компьютерной сети.

Структура экзаменационного билета.
Экзаменационный билет включает в себя два теоретических вопроса и одну задачу.
Примерные вопросы для экзамена:
1. Теоретический вопрос.
2. Теоретический вопрос.
3. Задач

Образец экзаменационного билета

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
Институт истории и государственного управления

Направление 10.05.05 «Безопасность информационных технологий»

Дисциплина Защита информационных процессов в компьютерных сетях

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. Мобильная связь третьего поколения 3G. Технология UMTS.
2. Стандартизация в связи.
3. Нарисовать структуру сети на базе рекомендации H.323, содержащую з аналоговых ТА, 3 компьютерных терминала, 3 зоны, 1 оператора. Пояснить взаимодействие устройств.

Зав. кафедрой управления информационной безопасностью А.С. Исмагилова

Кафедра управления информационной безопасностью

Критерии и методика оценивания (в баллах):

- 25-30 баллов выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок;

- 17-24 баллов выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки;

- 10-16 баллов выставляется студенту, если при ответе на теоретические вопросы студентом допущено несколько существенных ошибок в толковании основных понятий. Логика и полнота ответа страдают заметными изъянами. Заметны пробелы в знании основных методов. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос. Студент не решил задачу или при решении допущены грубые ошибки;

- 1-10 баллов выставляется студенту, если ответ на теоретические вопросы свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Обнаруживается отсутствие навыков применения теоретических знаний при выполнении практических заданий. Студент не смог ответить ни на один дополнительный вопрос.

Перевод оценки из 100-балльной в четырехбалльную производится следующим образом:

- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов);
- хорошо – от 60 до 79 баллов;
- удовлетворительно – от 45 до 59 баллов;
- неудовлетворительно – менее 45 баллов.

5. Учебно-методическое и информационное обеспечение дисциплины

5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины

Основная литература:

1. 1. Спицын В.Г.Информационная безопасность вычислительной техники: учебное пособие. - Томск: Эль Контент, 2011. – 148 с.

2. Аверченков В.И., Рытов М.Ю., Кондрашин Г.В., Рудановский М.В.Системы защиты информации в ведущих зарубежных странах: учебное пособие для вузов. - М.: Флинта, 2011. – 224 с.

3. Фефилов А.Д.Методы и средства защиты информации в сетях. - М.: Лаборатория книги, 2011. – 103 с.

Дополнительная литература

4. Гуц А.К., Вахний Т.В.Теория игр и защита компьютерных систем. - Омск: Омский государственный университет, 2013. – 160 с.

5. Заика А. Компьютерная безопасность. - М.: Рипол Классик, 2013. – 160 с.

6. Андрончик А.Н., Коллеров А.С., Синадский Н.И., Щербаков М.Ю.Сетевая защита на базе технологий фирмы CiscoSystems. Практический курс: учебное пособие. - Екатеринбург: Издательство Уральского университета, 2014. – 179 с.

7. Характеристика и особенности локальных компьютерных сетей. - М.: Лаборатория книги, 2012. – 157 с.

8. Никифоров С.В. Введение в сетевые технологии: Элементы применения и администрирования сетей: учебное пособие. - М.: Финансы и статистика, 2007. – 224 с.

9. Павлюк В.Д. Типовые топологии вычислительных сетей. - М.: Лаборатория книги, 2011. – 105 с.

5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы

1. Электронная библиотечная система БашГУ – www.bashlib.ru
2. Электронная библиотечная система «ЭБ БашГУ» - https://elib.bashedu.ru/
3. Электронная библиотечная система «Университетская библиотека онлайн» - https://biblioclub.ru/
4. Электронная библиотечная система издательства «Лань» - https://e.lanbook.com/
5. Электронный каталог Библиотеки БашГУ - http://www.bashlib.ru/catalogi/ -

6.Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
1. ***учебная аудитория для проведения занятий лекционного типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516	Лекции, практические занятия, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт.

(гуманитарный корпус). **2.** ***учебная аудитория для проведения лабораторных работ:*** компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус), лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507 (гуманитарный корпус). **3.** ***учебная аудитория для проведения занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 510 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **4.** ***учебная аудитория для курсового проектирования (выполнения курсовых работ):***аудитория № 613 (аудиторный корпус). **5.** ***учебная аудитория для проведения групповых и индивидуальных консультаций, учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус),		**Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 510** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 610** Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м. **Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507** Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технические средства обработки информации, стенд "Устройство ПК". **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404**

аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 510 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **6.*помещения для самостоятельной работы:***аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус). **7.*помещение для хранения и профилактического обслуживания учебного оборудования:*** аудитория № 523 (гуманитарный корпус).		Учебная мебель, компьютеры -15 штук. **Аудитория 402 читальный зал библиотеки** Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные. **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт. 1. Windows 8 Russian Russian OLP NL AcademicEditionи Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензиибессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License. Лицензии бессрочные.

Приложение 1

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины **Защита информационных процессов в компьютерных сетях**на 7 семестр
очная форма обучения

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	3ЗЕТ / 108 часа
Учебных часов на контактную работу с преподавателем:	55,2
лекций	18
практические	36
лабораторные	-
Других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	0,2
Учебных часов на самостоятельную работу обучающихся, включая подготовку к экзамену / зачету	53,8

Форма контроля: Зачет 7 семестр

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ
дисциплины **Защита информационных процессов в компьютерных сетях**на 8 семестр
очная форма обучения

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	49,2
лекций	16
практические	32
лабораторные	-
Других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	1,2
Учебных часов на самостоятельную работу обучающихся, включая подготовку к экзамену / зачету	67,8

Форма контроля: Экзамен 8 семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / Сем	ЛР	СРС		
1	2	3	4	5	6	7	8
1.	Основные понятия информационной безопасности, связанные с защитой информации в компьютерных сетях	9	20	-	43,8	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников. Выполнение практической работы	Тесты, КСР
2.	Защищенные компьютерные сети	9	16	-	20	Самостоятельное изучение рекомендуемой основной и дополнительной литературы выполнение рефератов	Устный опрос
	Всего часов	34	68	-	121,6		