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

Утверждено
на заседании кафедры
протокол № 7 от «18» февраля 2022 г.
Зав. кафедрой _____ / Исмагилова А.С.

Согласовано
Председатель УМК института


/ Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Защита информационных процессов в компьютерных системах
Обязательная часть

программа специалитета

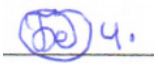
Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Специализация
Организация и технологии защиты информации (по отраслям)

Квалификация
Специалист по защите информации

Форма обучения
Очная

Разработчик (составитель)
Ассистент


/ Белова Е. П.

Для приема 2022 г.

Уфа - 2022 г.

Составитель: Белова Елена Петровна

Рабочая программа дисциплины утверждена на заседании кафедры управления информационной безопасностью, протокол №7 от «18» февраля 2022 г.

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/

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
2. Цель и место дисциплины в структуре образовательной программы
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)
4. Фонд оценочных средств по дисциплине

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

   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.
5. Учебно-методическое и информационное обеспечение дисциплины

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

   5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

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 (при наличии ОПК)	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
	ПК-2 - Способен проводить мероприятия по оценке защищенности компьютерных систем и сетей.	ПК-2.1 Знать основные критерии оценки защищенности компьютерных систем и сетей.	Знает основные критерии оценки защищенности компьютерных систем и сетей.
		ПК-2.2 Уметь выявлять и анализировать уязвимости.	Умеет выявлять и анализировать уязвимости.
		ПК-2.3 Владеть методами и инструментами оценки защищенности компьютерных систем и сетей.	Владеет методами и инструментами оценки защищенности компьютерных систем и сетей.
	ПК-3 - Способен анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации.	ПК-3.1 Знать основные задачи администрирования подсистемы ИБ объекта защиты; инструменты администрирования.	Знает основные задачи администрирования подсистемы ИБ объекта защиты; инструменты администрирования.
		ПК-3.2 Уметь выявлять и анализировать уязвимости.	Умеет выявлять и анализировать уязвимости.
		ПК-3.3 Владеть методами и инструментами оценки эффективности применяемых средств защиты информации.	Владеет методами и инструментами оценки эффективности применяемых средств защиты информации.
	ПК-1 - Способен формировать требования по защите информации и политики безопасности компьютерных	ПК-1.1 Знать средства администрирования ПАСЗИ.	Знает средства администрирования ПАСЗИ.
		ПК-1.2 Уметь работать с нормативно-правовой базой.	Умеет работать с нормативно-правовой базой.

	систем и сетей.	ПК-1.3 Владеть навыками формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Владеет навыками формирования требований по защите информации и политики безопасности компьютерных систем и сетей.

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Защита информационных процессов в компьютерных системах» относится к части, формируемой участниками образовательных отношений.
Дисциплина изучается на 5 курсе в 1 и 2 семестрах.
Целью учебной дисциплины «Защита информационных процессов в компьютерных системах» является формирование у студентов знаний и умений по защите технологий на объектах информатизации с использованием современных законодательных, инженерно-технических, криптографических и экономических методов.

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

ПК-2 - Способен проводить мероприятия по оценке защищенности компьютерных систем и сетей

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ПК-2.1 Знать основные критерии оценки защищенности компьютерных систем и сетей.	Знать основные критерии оценки защищенности компьютерных систем и сетей.	Не знает основные критерии оценки защищенности компьютерных систем и сетей.	Имеет отдалённые представления об основных критериях оценки защищенности компьютерных систем и сетей.	Знает большинство основных критериев оценки защищенности компьютерных систем и сетей.	Знает основные критерии оценки защищенности компьютерных систем и сетей.

ПК-2.2 Уметь выявлять и анализировать уязвимости.	Уметь выявлять и анализировать уязвимости.	Не умеет выявлять и анализировать уязвимости.	Имеет представления о выявлении и анализе уязвимости.	Частично умеет выявлять и анализировать уязвимости.	Умеет выявлять и анализировать уязвимости.
ПК-2.3 Владеть методами и инструментами оценки защищенности компьютерных систем и сетей.	Владеть методами и инструментами оценки защищенности компьютерных систем и сетей.	Не владеет методами и инструментами оценки защищенности компьютерных систем и сетей.	Имеет представления о методах и инструментах оценки защищенности компьютерных систем и сетей.	Частично владеет методами и инструментами оценки защищенности компьютерных систем и сетей.	Владеет методами и инструментами оценки защищенности компьютерных систем и сетей.

ПК-3 - Способен анализировать защищенность компьютерных систем, проводить проверку работоспособности и эффективности применяемых средств защиты информации

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ПК-3.1 Знать основные задачи администрирования подсистемы ИБ объекта защиты; инструменты администрирования.	Знать основные задачи администрирования подсистемы ИБ объекта защиты; инструменты администрирования.	Не знает основные задачи администрирования подсистемы ИБ объекта защиты; инструменты администрирования.	Имеет отдалённые представления об основных задачах администрирования подсистемы ИБ объекта защиты; инструментах администрирования.	Знает большинствоосновных задач администрирования подсистемы ИБ объекта защиты; инструментов администрирования.	Знает основные задачи администрирования подсистемы ИБ объекта защиты; инструменты администрирования.
ПК-3.2 Уметь выявлять и	Уметь выявлять и анализировать уязвимости.	Не умеет выявлять и анализировать уязвимости.	Имеет представления о выявлении и анализе уяз-	Частично умеет выявлять и анализировать уяз-	Умеет выявлять и анализировать уязвимости.

анализировать уязвимости.			вимостей.	вимости.	
ПК-3.3 Владеть методами и инструментами оценки эффективности применяемых средств защиты информации.	Владеть методами и инструментами оценки эффективности применяемых средств защиты информации.	Не владеет методами и инструментами оценки эффективности применяемых средств защиты информации.	Имеет смутные представления о методах и инструментах оценки эффективности применяемых средств защиты информации.	Частично владеет методами и инструментами оценки эффективности применяемых средств защиты информации.	Владеет методами и инструментами оценки эффективности применяемых средств защиты информации.

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

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ПК-1.1 Знать средства администрирования ПАСЗИ.	Знать средства администрирования ПАСЗИ.	Не знает средства администрирования ПАСЗИ.	Имеет отдалённые представления о средствах администрирования ПАСЗИ.	Знает большинство средств администрирования ПАСЗИ.	Знает средства администрирования ПАСЗИ.
ПК-1.2 Уметь работать с нормативно-правовой базой.	Уметь работать с нормативно-правовой базой.	Не умеет работать с нормативно-правовой базой.	Имеет представления о работе с нормативно-правовой базой.	Частично умеет работать с нормативно-правовой базой.	Умеет работать с нормативно-правовой базой.

ПК-1.3 Владеть навыками формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Владеть навыками формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Не владеет навыками формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Имеет смутные представления о навыках формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Частично владеет навыками формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Владеет навыками формирования требований по защите информации и политики безопасности компьютерных систем и сетей.

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей, перечисленных в рейтинг-плане дисциплины (для экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания для экзамена:

от 45 до 59 баллов – «удовлетворительно»;

от 60 до 79 баллов – «хорошо»;

от 80 баллов – «отлично».

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-2 - Способен проводить мероприятия по оценке защищенности компьютерных систем и сетей.	Знать основные критерии оценки защищенности компьютерных систем и сетей.	Аудиторная работа, тесты, устный опрос.
	Уметь выявлять и анализировать уязвимости.	Аудиторная работа, тесты, устный опрос.
	Владеть методами и инструментами оценки защищенности компьютерных систем и сетей.	Аудиторная работа, тесты, устный опрос.
ПК-3 - Способен анализировать защищенность компьютерных систем,	Знать основные задачи администрирования подсистемы ИБ объекта за-	Аудиторная работа, тесты, устный опрос.

проводить проверку работоспособности и эффективности применяемых средств защиты информации.	щиты; инструменты администрирования.	
	Уметь выявлять и анализировать уязвимости.	Аудиторная работа, тесты, устный опрос.
	Владеть методами и инструментами оценки эффективности применяемых средств защиты информации.	Аудиторная работа, тесты, устный опрос.
ПК-1 - Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей.	Знать средства администрирования ПАСЗИ.	Аудиторная работа, тесты, устный опрос.
	Уметь работать с нормативно-правовой базой.	Аудиторная работа, тесты, устный опрос.
	Владеть навыками формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Аудиторная работа, тесты, устный опрос.

Рейтинг-план

дисциплины «Защита информационных процессов в компьютерных системах»

Виды учебной деятельности	**Балл за конкретное задание**	**Число заданий за семестр**	**Баллы**	
			Минимальный	**Максимальный**
Модуль 1. Характеристика и основы принципы защиты информационных систем и информационных процессов				
Текущий контроль			**0**	35
1. Аудиторная работа	5	6	0	30
2. Устный опрос	1	5	0	5
Рубежный контроль			**0**	10
1.Тесты	1	10	0	10
Модуль 2. Стандарты по защите информации и информационных процессов, её организация и средства				
Текущий контроль			**0**	35
1. Аудиторная работа	5	6	0	30
2. Устный опрос	1	5	0	5
Рубежный контроль			**0**	10
1.Тесты	1	10	0	10
Поощрительные баллы				
1. Студенческая олимпиада, участие в конференциях	5			5
2. Публикация статей	5			5
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
Посещение лекционных занятий			0	–6
2. Посещение практических (семинарских, лабора-			0	–10

торных занятий)				
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.

Обучающийся излагает содержание вопроса изученной темы.

Критерии и методика оценивания:

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

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

- 3 балла выставляется обучающемуся, 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 обучающемуся, если точно используется специализированная терминология, показано уверенное владение нормативной базой;

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

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

Зачёт и Экзамен

Зачёт проводится в 9 семестре.

Экзамен проводится в 10 семестре. Экзаменационный билет содержит 2 теоретических вопроса.

Типовые вопросы к зачёту и экзамену:

1. Основы безопасности сетевых информационных технологий.
2. IP-сеть организации.
3. Классификация уязвимостей и атак в компьютерных сетях.
4. Защитные механизмы и средства обеспечения безопасности в компьютерных сетях.
5. Базовые принципы сетевого взаимодействия. Модель OSI. Архитектура TCP/IP.
6. Безопасность физического и канального уровней модели OSI.
7. Сетевые анализаторы и «снифферы».
8. Проблемы безопасности протокола разрешения адресов ARP.
9. Безопасность сетевого уровня модели OSI. Меры защиты сетевого уровня.
10. Приведите примеры того, как злоумышленник может воспользоваться информацией из заголовка IP.
11. Протоколы IP и ICMP.

12. Протокол IPSec.Транспортный и туннельный режимы IPSec.
13. Безопасность транспортного уровня модели OSI. Протоколы TCP и UDP. Меры защиты транспортного уровня.
14. Проблемы безопасности протоколов прикладного уровня (Telnet, FTP, HTTP, SMTP).
15. Понятие о моделях безопасности ОС.
16. Варианты решений по обеспечению безопасности сети организации.
17. Применение межсетевых экранов для защиты корпоративных сетей.
18. Место и роль межсетевых экранов в корпоративных сетях. Типовая корпоративная сеть.
19. Понятие межсетевых экранов. Защитные механизмы, реализуемые межсетевыми экранами.
20. Обзор документов RFC, имеющих отношение к межсетевым экранам, основные термины и определения. Типы межсетевых экранов.
21.Фильтрация пакетов. Параметры фильтрации. Правила фильтрации. Реализация пакетных фильтров.
22. Понятие демилитаризованной зоны.
23. Особенности фильтрации различных типов трафика.
24. Пакетный фильтр на базе ОС Windows.
25. Шлюзы. Трансляция адресов. Типы трансляции.
26. Шлюзы прикладного уровня, варианты конфигурации.
27. Расположение межсетевых экранов в корпоративной сети.
28. Особенности фильтрации служб прикладного уровня DNS, FTP, SMTP.
29. Противодействие сетевым атакам при помощи межсетевых экранов.
30. Интеграция межсетевых экранов с другими средствами защиты.
31. Достоинства и недостатки межсетевых экранов как средств защиты.
32. Место и роль криптографии в обеспечении безопасности компьютерных сетей.
33.Актуальность проблемы безопасности сетевых технологий.
34.Место и роль криптографических методов и средств в системах управления и электронной коммерции.
35. Задачи, решаемые средствами криптографической защиты информации: обеспечение конфиденциальности, целостности и аутентичности данных, разграничение ответственности, аутентификация абонентов.
36. Электронные цифровые подписи. Механизмы цифровой подписи.
37. Техника контроля использования асимметричных ключей.
38. Концепция инфраструктуры открытых ключей (PublicKeyInfrastructure —PKI). Основные термины и определения. Компоненты PKI и их функции: орган сертификации, органы регистрации, владельцы сертификатов, клиенты и клиентское программное обеспечение, хранилище сертификатов.
39. Модели доверия при наличии различных органов сертификации. Цепочки сертификатов и сертификационные пути. Доверие с разделенными доменами.
40. Какие существуют методы оценки защищенности компьютерной сети?
41. Перечислить и описать разновидности биометрических систем идентификации личности.
42. Описать принцип аналитического метода оценки защищенности компьютерной сети.
43. Описать принцип имитационного метода оценки защищенности компьютерной сети.
44. Перечислить основные правила обеспечения политики безопасности информации в компьютерных сетях.
45. Частные и виртуальные частные сети.
46. Классификация VPN.
47. Какие технологии в сетях VPN используются, чтобы обеспечить безопасность в компьютерных сетях?
48. Защита удаленного доступа.
49. Аудит и мониторинг безопасности компьютерных сетей.
50. Стандарты информационной безопасности

Критерии оценивания результатов экзамена: При выставлении баллов именно за экзамен (до 30 баллов в дополнение к баллам, полученным за другие виды отчетности) действует такой критерий оценки:

25-30 баллов

Студент дал полные, развернутые ответы на теоретический вопрос билета и правильно выполнил практическое задание, продемонстрировал знание функциональных возможностей, терминологии, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок.

17-24 баллов

Студент раскрыл в основном теоретический вопрос, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности. При выполнении практической части работы допущены несущественные ошибки, но все задание выполнено до конца.

10-16 баллов

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. Теоретические вопросы в целом изложены достаточно, но с пропусками материала. Имеются принципиальные ошибки в логике построения ответа на вопрос. Студент сделал практическое задание лишь частично.

1-10 баллов

Ответ на теоретический вопрос свидетельствует о непонимании и крайне неполном знании основных понятий и методов. Студент не смог ответить ни на один дополнительный вопрос. При этом студент не решил задачу или лишь частично (на ½ от задания).

Перевод оценки из 100-балльной в 4-балльную 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.

Типовая контрольная работа

Содержание работы.

Для локальной сети, согласно вашему варианту, разработать модель угроз и нарушителя безопасности.

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;

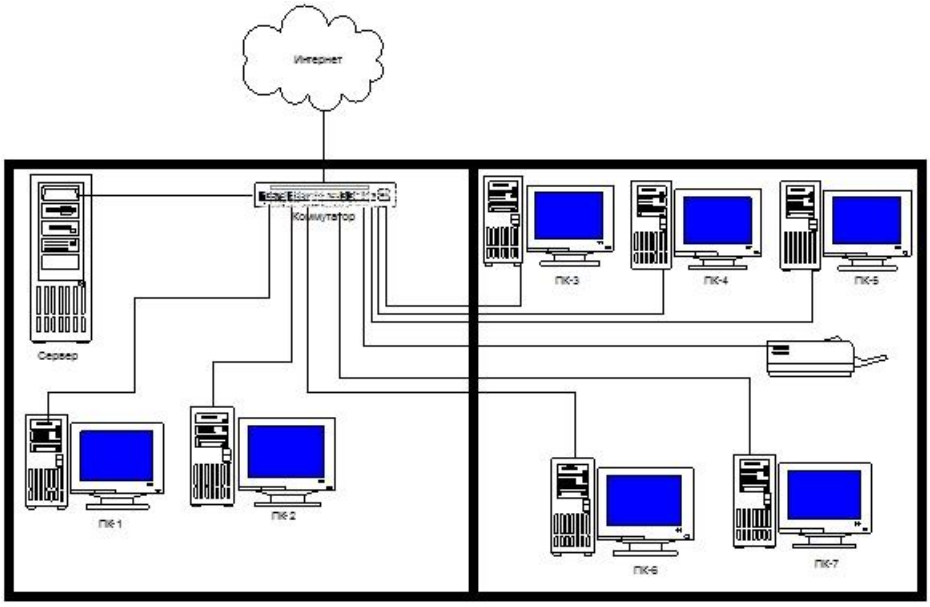
5 – й этап. Определяется система защиты с набором барьеров;

6 – й этап. Определяется возможные затраты при реализации различных угроз и их комбинаций –

строится дерево сценариев.

Вариант 1

ЛВС небольшого торгового предприятия.



Типовые тестовые вопросы

1. В число универсальных сервисов безопасности входят:
1) шифрование;
2) средства построения виртуальных частных сетей;
3) туннелирование.

2. Комплексное экранирование может обеспечить:
1) разграничение доступа по сетевым адресам;
2) выборочное выполнение команд прикладного протокола;
3) контроль объема данных, переданных по TCP-соединению.

3. Уровень безопасности С, согласно "Оранжевой книге", характеризуется:
1) произвольным управлением доступом;
2) принудительным управлением доступом;
3) верифицируемой безопасностью.

4. Перехват данных является угрозой:
1) доступности;
2) конфиденциальности;
3) 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;
3) 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 незапрошенной рекламной информации.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература:

1. Спицын В.Г.Информационная безопасность вычислительной техники: учебное пособие. Томск: Эль Контент, 2011. – 148 с.
http://biblioclub.ru/index.php?page=book&id=208694&sr=1
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.
http://biblioclub.ru/index.php?page=book&id=93351&sr=1
3. Фефилов А.Д.Методы и средства защиты информации в сетях. - М.: Лаборатория книги, 2011. – 103 с.
http://biblioclub.ru/index.php?page=book&id=140796&sr=1

Дополнительная литература:

1. Гуц А.К., Вахний Т.В.Теория игр и защита компьютерных систем. - Омск: Омский государственный университет, 2013. – 160 с.http://biblioclub.ru/index.php?page=book&id=237190&sr=1
2. Заика А.Компьютерная безопасность. - М.: Рипол Классик, 2013. – 160 с. http://biblioclub.ru/index.php?page=book&id=227317&sr=1
3. 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. http://biblioclub.ru/index.php?page=book&id=275694&sr=1
4. Характеристика и особенности локальных компьютерных сетей. - М.: Лаборатория книги, 2012. – 157 с. http://biblioclub.ru/index.php?page=book&id=142934&sr=1
5. Никифоров С.В. Введение в сетевые технологии: Элементы применения и администрирования сетей: учебное пособие. - М.: Финансы и статистика, 2007. – 224 с. http://biblioclub.ru/index.php?page=book&id=221461&sr=1
6. Павлюк В.Д. Типовые топологии вычислительных сетей. - М.: Лаборатория книги, 2011. –

http://biblioclub.ru/index.php?page=book&id=142528&sr=1

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 «Университетская библиотека онлайн» – https://biblioclub.ru.
2. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
3. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
4. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
5. http://univertv.ru/video/matematika/ – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
6. www.newlibrary.ru – Новая электронная библиотека;
7. www. edu.ru – Федеральный портал российского образования;
8. www.elibrary.ru – Научная электронная библиотека;
9. www.nehudlit.ru – Электронная библиотека учебных материалов.
10. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
11. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
12. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

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

Наименование специальных помещений и помещений для самостоятельной работы	***Вид занятий***	***Наименование оборудования, программного обеспечения***
1	**2**	**3**
Аудитория № 516	Лекции, семинары, практические занятия.	Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование.
Аудитория № 610	Лекции, семинары, практические занятия.	Учебная мебель, доска, LED Телевизор TCLL55P6 US-BLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м.
Аудитория № 609	Лекции, семинары, практические занятия.	Учебная мебель, доска, мобильное мультимедийное оборудование.
Аудитория № 608	Лекции, семинары, практические занятия.	Учебная мебель, доска, мобильное мультимедийное оборудование
Аудитория № 613	Практические занятия, лабораторные работы.	Учебная мебель, доска, моноблок стационарный – 12 шт. с возможностью подключения к сети Интернет и

		доступа в электронную информационно-образовательную среду. Windows 8 Russian Windows Professional 8 Russian Upgrade. Договор №104 от 17.06.2013 г. Лицензии бессрочные. Microsoft Office Standard 2013 Russian. Договор №114 от 12.11.2014 г. Лицензии бессрочные.

Приложение 1

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

Содержание рабочей программы
дисциплины «Защита информационных процессов в компьютерных системах»
на 9 семестр ОФО

Вид работы	**Объем дисциплины**
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	54,2
лекций	18
практических/ семинарских	36
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	20

Форма контроля:
Зачет 9 семестр

Содержание рабочей программы
дисциплины «Защита информационных процессов в компьютерных системах»
на 10 семестр ОФО

Вид работы	**Объем дисциплины**
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	51,2
лекций	16
практических/ семинарских	32
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	3,2
Учебных часов на самостоятельную работу обучающихся (СР)	20
из них, предусмотренные на выполнение курсовой работы / курсового проекта	2
Учебных часов на подготовку к зачету (Контроль)	27

Форма контроля:
Экзамен 10 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	СР		
1	2	3	4	5	6	7	8
1.	**Модуль 1. Характеристика,основы и принципы защиты информационных систем и информационных процессов:** **Раздел 1. Введение в дисциплину.** **Характеристика информационных систем и информационных процессов:** 1.1 Общая характеристика информационные технологии и информационные системы. Примеры информационных технологий. 1.2. Государственные стандарты на разработку и создание информационных систем. **Раздел 2. Основы принципы защиты информационных процессов в компьютерных систе-**	8	21	22	20	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Аудиторная работа, тесты

	мах: 2.1. Основные угрозы информации в компьютерных системах. Ценности, опасности, потери, риски, угрозы в компьютерных системах. Основные угрозы информации в компьютерных системах; специфика возникновения угроз в открытых сетях; особенности защиты информации на узлах компьютерной сети; системные вопросы защиты программ и данных. 2.2. Анализ рисков. 2.3 Модель противника, возможности противника; параллельный анализ целей и возможностей злоумышленника в компьютерной сети и в ситуации при наличии изолированного компьютера. Анализ критических технологий. 2.4. Политика безопасности для компьютерных систем. 2.5. Государственная политика в области безопасности ИП в компью-						

	терных системах. 2.6. Основные категории требований к программной и программно-аппаратной реализации средств защиты ИП. 2.7. Система лицензирования и сертификации средств защиты ИП. 2.8. Аттестация защищенных систем. Структуры в РФ, обеспечивающие лицензирование и сертификацию. Нормативная база и ответственность за защиту ИП в компьютерных системах. Руководящий документ Гостехкомиссии по оценке защищенности АС. Стандарты по защите информации и информационных процессов.						
2.	**Модуль 2. Стандарты по защите информации и информационных процессов, её организация и средства** **Раздел 3. Стандарты по защите информации и информационных процессов:** 3.1. Стандарт США «Розовая книга». Построение	8	21	22	20	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Аудиторная работа, тесты

	гарантированно защищенных баз данных и их оценка по стандарту «Оранжевая книга». 3.2 Европейский стандарт по безопасности ИТ. Стандарт ITSEC. Критерии оценки защищенности ИП. Функциональные требования. Вопросы гарантий и эффективности. **Раздел 4. Организация и средства защиты информационных процессов в компьютерных системах:** 4.1 Базовые концепции безопасности ИП в компьютерных системах. Профиль защиты. Функции поддержки политики безопасности. Гарантии безопасности. Требования по безопасности информационных технологий. Оценки защищенности. Компоненты подсистем поддержки политики безопасности. 4.2. Требования к подсистемам аудита ИП. Подсистемы подтверждения подлинности отправки и получения со-						

	общения. Подсистемы разграничения доступа. Подсистемы аутентификации. Подсистемы защиты функций защиты. Подсистемы защиты ресурсов системы. Подсистемы защиты связи. 4.3. Гарантии безопасности ИП в компьютерных системах. Уровни гарантий. Методология анализа гарантий. 4.4.Каналы утечки и их анализ. 4.5. Управление конфигурацией. Безопасная установка систем защиты информационных процессов. 4.6. Безопасная модернизация информационных процессов в компьютерных системах.						
	Всего часов	16	42	44	119,6		