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

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

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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Дисциплина
Программно-аппаратная защита информации

Обязательная часть (Б1.О.22)

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

Разработчик (составитель) . _____ .	_____ / Салов И.В.

Для приема: 2021 г.

Уфа 2021 г.

Составитель: Салов Игорь Владимирович

Рабочая программа дисциплины *утверждена* на заседании кафедры 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 / Исмагилова А.С. /

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

Заведующий кафедрой _____/ Исмагилова А.С. /

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 (при наличии ОПК)	**Формируемая компетенция (с указанием кода)**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения по дисциплине**
Системное и критическое мышление	УК-1 Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	УК-1.1 Знает основные принципы и методы осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.	Знать основные принципы и методы осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.
		УК-1.2 Умеет осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	Уметь осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.
		УК-1.3 Владеет применением основных принципов и методов осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.	Владеть применением основных принципов и методов осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.
Проектно-технологические	ОПК-7. Способен применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач	ОПК-7.1 Знает программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.	Знать программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.
		ОПК-7.2 Умеет применять программные средства	Уметь применять программные средства системного и

		системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.	прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.
		ОПК-7.3 Владеет программными средствами системного и прикладного назначения, языками, методами и инструментальными средствами программирования для решения профессиональных задач.	Владеть программными средствами системного и прикладного назначения, языками, методами и инструментальными средствами программирования для решения профессиональных задач.

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Программно-аппаратная защита информации» относится к обязательной части.

Дисциплина изучается на 3 курсе в 5,6 семестрах.

Целью учебной дисциплины «Программно-аппаратная защита информации», является формирование навыков применения программных средств системного и прикладного назначения, языков, методов и инструментальных средств программирования для решения задач информационной безопасности.

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.

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено

УК-1.1 Знает основные принципы и методы осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.	Знать основные принципы и методы осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.	Не знает или показывает очень слабые знания.	Знает основные принципы и методы осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.
УК-1.2 Умеет осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	Уметь осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	Не умеет.	Умеет осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.
УК-1.3 Владеет применением основных принципов и методов осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.	Владеть применением основных принципов и методов осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.	Не владеет.	Владеет применением основных принципов и методов осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Неудовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
УК-1.1 Знает основные принципы и методы осуществления	Знать основные принципы и методы осуществления критического анализа	Не знает или показывает	Знает некоторые основные	Знает некоторые основны	Знает основные принцип

критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.	проблемных ситуаций на основе системного подхода и выработки стратегии действий.	очень слабые знания.	принципы и методы осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий, но делает ошибки при их использовании.	е принципы и методы осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.	ы и методы осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.
УК-1.2 Умеет осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	Уметь осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	Не умеет.	Умеет осуществлять критический анализ основных проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий, но делает при этом ошибки	Умеет осуществлять критический анализ основных проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	Умеет осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.
УК-1.3 Владеет применением основных принципов и	Владеть применением основных принципов и методов осуществления критического анализа	Не владеет.	Владеет применением некоторых	Владеет применением некоторых	Владеет применением основных

методов осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.	проблемных ситуаций на основе системного подхода и выработки стратегии действий.		основных принципов и методов осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий, но делает ошибки при их использовании.	основных принципов и методов осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.	принципов и методов осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.

ОПК-7. Способен применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ОПК-7.1 Знает программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.	Знать программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.	Не знает или показывает очень слабые знания.	Знает основные программные средства системного и прикладного назначения, методы и инструментальные средства программирования,	Знает основные программные средства системного и прикладного назначения, методы и инструментальные средства программирования,	Знает программные средства системного и прикладного назначения, методы и инструментальные средства программирования, использу

			используемые для решения профессиональных задач, но делает ошибки при их выборе.	используемые для решения профессиональных задач.	емые для решения профессиональных задач.
ОПК-7.2 Умеет применять программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.	Уметь применять программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.	Не умеет.	Умеет применять основные программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач, но делает ошибки при их использовании.	Умеет применять основные программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.	Умеет применять программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.
ОПК-7.3 Владеет программными средствами системного и прикладного назначения, языками, методами и инструментальными средствами программирования для решения профессиональных задач.	Владеть программными средствами системного и прикладного назначения, языками, методами и инструментальными средствами программирования для решения профессиональных задач.	Не владеет.	Владеет основными программными средствами системного и прикладного назначения, языками,	Владеет основными программными средствами системного и прикладного назначения, языками,	Владеет программными средствами системного и прикладного назначения, языками, методами и

			методами и инструментальными средствами программирования для решения профессиональных задач, но делает ошибки при их использовании.	методами и инструментальными средствами программирования для решения профессиональных задач.	инструментальными средствами программирования для решения профессиональных задач.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ОПК-7.1 Знает программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.	Знать программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.	Не знает или показывает очень слабые знания.	Знает программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.
ОПК-7.2 Умеет применять программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.	Уметь применять программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.	Не умеет.	Умеет применять программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.
ОПК-7.3 Владеет программными средствами	Владеть программными средствами системного и прикладного назначения, языками, методами и	Не владеет.	Владеет программными средствами системного и

системного и прикладного назначения, языками, методами и инструментальными средствами программирования для решения профессиональных задач.	инструментальными средствами программирования для решения профессиональных задач.		прикладного назначения, языками, методами и инструментальными средствами программирования для решения профессиональных задач.

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

УК-1. Способен осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
УК-1.1 Знает основные принципы и методы осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.	Знать основные принципы и методы осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.	тестирование, практическое задание; лабораторная работа
УК-1.2 Умеет осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	Уметь осуществлять критический анализ проблемных ситуаций на основе системного подхода, вырабатывать стратегию действий.	тестирование, практическое задание; лабораторная работа
УК-1.3 Владеет применением основных принципов и методов осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.	Владеть применением основных принципов и методов осуществления критического анализа проблемных ситуаций на основе системного подхода и выработки стратегии действий.	тестирование, практическое задание; лабораторная работа

ОПК-7. Способен применять программные средства системного и прикладного назначения, языки, методы и инструментальные средства программирования для решения профессиональных задач.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ОПК-7.1 Знает программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.	Знать программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.	тестирование, практическое задание; лабораторная работа
ОПК-7.2 Умеет применять программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.	Уметь применять программные средства системного и прикладного назначения, методы и инструментальные средства программирования, используемые для решения профессиональных задач.	тестирование, практическое задание; лабораторная работа
ИПК-7.3 Владеет программными средствами системного и прикладного назначения, языками, методами и инструментальными средствами программирования для решения профессиональных задач.	Владеть программными средствами системного и прикладного назначения, языками, методами и инструментальными средствами программирования для решения профессиональных задач.	тестирование, практическое задание; лабораторная работа

Критериями оценивания при модульно-рейтинговой системе являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для экзамена: текущий контроль – максимум 40 баллов; рубежный контроль – максимум 30 баллов, поощрительные баллы – максимум 10; для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 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».

для зачета:

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

не зачтено – от 0 до 59 рейтинговых баллов).

Рейтинг – план дисциплины
«Программно-аппаратная защита информации»

Специальность: 10.05.05 Безопасность информационных технологий в правоохранительной сфере

курс 3, семестр 5

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Основные принципы программно-аппаратных средств обеспечения информационной безопасности.				
Текущий контроль			0	
Лабораторная работа	4	5	0	20
Практическая работа	4	5	0	20
Рубежный контроль				
Тест	10	1	0	10
Всего		4	0	50
Модуль 2. Классификация функциональных требований по защите информации и данных.				
Текущий контроль				
Лабораторная работа	5	4	0	20
Практическая работа	5	4	0	20
Рубежный контроль				
Тест	10	1	0	10
Всего		5	0	50
Поощрительные баллы				
1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции по профилю	3	1	0	3
Всего		3	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10
Итоговый контроль				
1. Зачет	60	1	60	100

курс 3, семестр 6

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 3. Программно-аппаратные средства защиты информации.				
Текущий контроль				
Лабораторная работа	4	4	0	16
Практическая работа	4	4	0	16
Рубежный контроль				
Тест	8	1	0	8
Всего			0	40
Модуль 4. Программно-аппаратные средства защиты информации при передаче по каналам связи.				

Текущий контроль				
Лабораторная работа	3	4	0	12
Практическая работа	3	4	0	12
Рубежный контроль				
Тест	6	1	0	6
Всего			0	30
Поощрительные баллы				
1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции по профилю	3	1	0	3
Всего		3	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10
Итоговый контроль				
1.Экзамен	30	1	0	30

Зачет

Вопросы для зачета:

1. Основные понятия и определения в области создания ПАСОИБ.
2. Нормативно-правовая база создания ПАСОИБ.
3. Анализ угроз информационной безопасности.
4. Анализ сетевых угроз информационной безопасности.
5. Классификация ПАСОИБ.
6. Функциональные возможности ПАСОИБ.
7. Принципы разработки ПАСОИБ.
8. Концепция диспетчера доступа.
9. Основные этапы проектирования ПАСОИБ.
10. Классификация функциональных требований по защите информации и данных.
11. Принципы действия и технологические особенности программно-аппаратных средств, реализующих отдельные функциональные требования по защите информации и данных и их взаимодействие с общесистемными компонентами вычислительных систем.
12. Методы обеспечения идентификации и аутентификации.
13. Методы криптографической защиты.
14. Методы и средства хранения ключевой информации.
15. Методы и средства ограничения доступа к компонентам вычислительных систем.
16. Характеристика методов и средства привязки программного обеспечения к аппаратному кружению и физическим носителям.
17. Методы аудита безопасности.
18. Методы обеспечения доступа к системе защиты и управления безопасностью.
19. Методы обеспечения целостности системы защиты.
20. Классификация аппаратных компонентов средств защиты программ.
21. Классификация программных компонентов средств защиты программ.
22. Структура программного обеспечения.

23. Способы встраивания средств защиты в программное обеспечение.
24. Способы определения факта незаконного использования программ.
25. Способы защиты программ от незаконного использования.
26. Способы изучения кода программ.
27. Способы защиты программ от изучения кода.
28. Основные принципы обеспечения безопасности программ.
29. Изолированная программная среда.
30. Классификация программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ.
31. Характеристики программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ.
32. Понятие электронного замка.
33. Принципы построения и функционирования электронных замков.
34. Механизмы контроля аппаратной конфигурации ПЭВМ.
35. Общие принципы разграничения доступа пользователей к устройствам ПЭВМ.
36. Основные принципы криптографической защиты информации.
37. Классификация программно-аппаратных средств защиты информации в сетях передачи данных.
38. Принципы построения и функционирования межсетевых экранов в сетях передачи данных.
39. Программно-аппаратные средства межсетевого экранирования.

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

Шкалы оценивания:

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

не зачтено – от 0 до 59 рейтинговых баллов).

Экзамен

Структура экзаменационного билета

Экзаменационный билет состоит из двух вопросов, отражающих соответственно материал первого и второго модуля.

Экзаменационные материалы

40. Основные понятия и определения в области создания ПАСОИБ.
41. Нормативно-правовая база создания ПАСОИБ.
42. Анализ угроз информационной безопасности.
43. Анализ сетевых угроз информационной безопасности.
44. Классификация ПАСОИБ.
45. Функциональные возможности ПАСОИБ.
46. Принципы разработки ПАСОИБ.
47. Концепция диспетчера доступа.
48. Основные этапы проектирования ПАСОИБ.
49. Классификация функциональных требований по защите информации и данных.
50. Принципы действия и технологические особенности программно-аппаратных средств, реализующих отдельные функциональные требования по защите информации и данных и их взаимодействие с общесистемными компонентами вычислительных систем.

51. Методы обеспечения идентификации и аутентификации.
52. Методы криптографической защиты.
53. Методы и средства хранения ключевой информации.
54. Методы и средства ограничения доступа к компонентам вычислительных систем.
55. Характеристика методов и средства привязки программного обеспечения к аппаратному кружению и физическим носителям.
56. Методы аудита безопасности.
57. Методы обеспечения доступа к системе защиты и управления безопасностью.
58. Методы обеспечения целостности системы защиты.
59. Классификация аппаратных компонентов средств защиты программ.
60. Классификация программных компонентов средств защиты программ.
61. Структура программного обеспечения.
62. Способы встраивания средств защиты в программное обеспечение.
63. Способы определения факта незаконного использования программ.
64. Способы защиты программ от незаконного использования.
65. Способы изучения кода программ.
66. Способы защиты программ от изучения кода.
67. Основные принципы обеспечения безопасности программ.
68. Изолированная программная среда.
69. Классификация программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ.
70. Характеристики программно-аппаратных средств защиты от несанкционированного доступа к информации, хранимой в ПЭВМ.
71. Понятие электронного замка.
72. Принципы построения и функционирования электронных замков.
73. Механизмы контроля аппаратной конфигурации ПЭВМ.
74. Общие принципы разграничения доступа пользователей к устройствам ПЭВМ.
75. Основные принципы криптографической защиты информации.
76. Классификация программно-аппаратных средств защиты информации в сетях передачи данных.
77. Принципы построения и функционирования межсетевых экранов в сетях передачи данных.
78. Программно-аппаратные средства межсетевого экранирования.
79. Основные принципы защиты информации при передаче по каналам связи.
80. Программно-аппаратные средства защиты информации при передаче по каналам связи.
81. Основные принципы разграничения доступа к сетевым ресурсам.
82. Основные принципы обнаружения сетевых атак.
83. Программно-аппаратные средства обнаружения сетевых атак.
84. Основные принципы защиты от сетевых атак.
85. Программно-аппаратные средства защиты от сетевых атак.
86. Основные принципы управления безопасностью сети.
87. Программно-аппаратные средства управления безопасностью сети.
88. Обзор штатных средств сетевого оборудования, предназначенных для защиты информации при передаче по каналам связи.
89. Способы применения штатных средств сетевого оборудования, предназначенных для защиты информации при передаче по каналам связи.
90. Основные требования к информационной безопасности.
91. Задачи сертификации программно-аппаратных средств на соответствие требованиям информационной безопасности.
92. Технология сертификации программно-аппаратных средств на соответствие

требованиям информационной безопасности.

93. Классификация требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности.
94. Проверка ОИ на базе вычислительной техники.
95. Электронный документ (ЭД). Понятие ЭД. Типы ЭД.
96. Виды информации в КС. Информационные потоки в КС. Понятие исполняемого модуля.
97. Уязвимость компьютерных систем. Понятие доступа, субъект и объект доступа.
98. Понятие несанкционированного доступа (НСД), классы и виды НСД. Несанкционированное копирование программ как особый вид НСД.
99. Понятие злоумышленника; злоумышленник в криптографии и при решении проблем компьютерной безопасности (КБ).
100. Политика безопасности в компьютерных системах. Оценка защищенности.
101. Способы защиты конфиденциальности, целостности и доступности в КС.
102. Руководящие документы Гостехкомиссии по оценке защищенности от НСД.
103. Понятие идентификации пользователя. Задача идентификации пользователя. Понятие протокола идентификации. Локальная и удаленная идентификация. Идентифицирующая информация (понятие, способы хранения, связь с ключевыми системами).
104. Файл как объект доступа. Оценка надежности систем ограничения доступа – сведение к задаче оценки стойкости.
105. Организация доступа к файлам. Иерархический доступ к файлам. Понятие атрибутов доступа. Организация доступа к файлам различных ОС.
106. Защита сетевого файлового ресурса на примерах организации доступа в различных ОС.
107. Способы фиксации факторов доступа. Журналы доступа и критерии их информативности.
108. Выявление следов несанкционированного доступа к файлам, метод инициированного НСД.
109. Доступ данных со стороны процесса (понятие; отличия от доступа со стороны пользователя).
110. Построение программно-аппаратных комплексов шифрования.
111. Аппаратные и программно-аппаратные средства криптозащиты данных. Построение аппаратных компонент криптозащиты данных, специализированные СБИС как носителя алгоритма шифрования.
112. Защита алгоритма шифрования; принцип чувствительной области и принцип главного ключа.
113. Необходимые и достаточные функции аппаратного средства криптозащиты. Проектирование модулей криптопреобразований на основе сигнальных процессов.
114. Классификация защищаемых компонент ПЭВМ: отчуждаемые и неотчуждаемые компоненты ПЭВМ.
115. Процесс начальной загрузки ПЭВМ, взаимодействие аппаратной и программной частей. Механизмы расширения BIOS. Преимущества и недостатки программных и аппаратных средств.
116. Способы защиты информации на съемных дисках. Организация прозрачного режима шифрования.
117. Магнитные диски прямого доступа.
118. Магнитные и интеллектуальные карты.
119. Средство TouchMemory.
120. Способы изучения ПО: статистическое и динамическое изучение. Роль

программной и аппаратной среды.

121. Временная надежность (невозможность обеспечения гарантированной надежности).
122. Задачи защиты от изучения и способы их решения.
123. Защита от отладки: итеративный программный замок.
124. Защита от отладки: принцип ловушек и избыточного кода.
125. Защита от дизассемблирования. Принцип внешней загрузки файлов.
126. Динамическая модификация программы. Защита от трассировки по прерываниям.
127. Способы ассоциирования защиты и программного обеспечения. Оценка надежности защиты от отладки.
128. Ключи на базе перепрограммируемой постоянной памяти.
129. Ключи на базе заказных чипов.
130. Примеры реализации ключей (Aktivator, HASP, Alladin и другие).
131. Ключи на базе микропроцессоров.
132. Модели взаимодействия прикладной программы и программы злоумышленника, компьютерные вирусы как особый класс РПВ, активная и пассивная защита, необходимые и достаточные условия недопущения разрушающего воздействия; понятие изолированной программной среды, защита программ от изменения и контроль целостности.
133. Основные категории требований к программной и программно-аппаратной реализации средств обеспечения информационной безопасности; программно-аппаратные средства обеспечения информационной безопасности в типовых ОС, СУБД, вычислительных сетях.

Пример экзаменационного билета:

Форма 1.4.-33

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ
КАФЕДРА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Дисциплина Программно-аппаратная защита информации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. 1. Основные понятия и определения в области создания ПАСОИБ.
2. Построение программно-аппаратных комплексов шифрования..

Зав. Кафедрой УИБ А.С. Исмагилова

Кафедра управления информационной безопасностью

Критерии оценивания результатов экзамена для ОФО:

Критерии оценки (в баллах):

- 25-30 баллов выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание терминологии, основных понятий, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы.

- 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.

- 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.

- 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.

Устанавливается следующая градация перевода оценки из многобалльной в четырехбалльную:

Экзамены:

- 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.

Примерная тематика курсовых проектов (работ)

Курсовое проектирование не предусмотрено

Тестовые задания

При изучении дисциплины используются тестовые задания закрытого типа. Каждое тестовое задание включает вопрос и варианты ответов к нему. Тестирование выполняется в письменной форме.
Необходимо выбрать один ответ из предложенных вариантов.

Модуль 1. Основные принципы программно-аппаратных средств обеспечения информационной безопасности.

1. Незаконный сбор, присвоение и передача сведений составляющих коммерческую тайну, наносящий ее владельцу ущерб, - это...
   1) политическая разведка;
   2) промышленный шпионаж;
   3) добросовестная конкуренция;
   4) конфиденциальная информация;
   5) правильного ответа нет.
2. Какая информация является охраняемой внутригосударственным законодательством или международными соглашениями как объект интеллектуальной собственности:
   1) любая информация;
   2) только открытая информация;

3) запатентованная информация;

4) закрываемая собственником информация;

5) коммерческая тайна.

6) Метод записи чисел, представление чисел с помощью письменных знаков;

7) Система измерения, сбора, анализа, представления и интерпретации информации о посетителях веб-сайтов с целью их улучшения и оптимизации.

3. Кто может быть владельцем защищаемой информации

а) только государство и его структуры;

б) предприятия акционерные общества, фирмы;

в) общественные организации;

г) только вышеперечисленные.

4. Какие сведения на территории РФ могут составлять коммерческую тайну

1) учредительные документы и устав предприятия;

2) сведенья о численности работающих, их заработной плате и условиях труда;

3) документы о платежеспособности, об уплате налогов, о финансово-хозяйственной деятельности;

4) другие;

5) любые.

5. Защита информации это-

1) потенциальная возможность неправомерного преднамеренного или случайного воздействия , приводящее к потере или разглашению информации.

2) реализация права на государственную тайну и конфиденциальную информацию

3) устранение или нейтрализация негативных источников, причин и условий воздействия на информацию

4) правовые, организационные и технические меры, направленные на обеспечение защиты информации

6. Каналы утечки информации- это

1) это комплексы специального технического и программного обеспечения, предназначенные для предотвращения утечки информации

2) методы и пути утечки информации из информационной системы

3) потенциальная возможность неправомерного преднамеренного или случайного воздействия

4) соблюдение конфиденциальности информации ограниченного доступа

7. Существуют следующие виды ПО (добавьте недостающее).

1) Прикладное ПО

2) Системное ПО

3) **Инструментальное ПО**

8. К функциям ОС относится :

2) поддержка работы всех программ, обеспечение их взаимодействия с аппаратурой

3) управление процессором путем чередования выполнения программ;

4)обработка прерываний и синхронизация доступа к ресурсам вычислительной системы;

5)управление памятью путем выделения программам на время их выполнения требуемой памяти;

9. Операционная система Windows является :

1) многозадачной

2) однозадачной

3) многопользовательской

4) однопользовательской

10. Атаки на ОС бывают:

1) Локальными

2) Глобальными

3) Удаленными

4) Близкими

11. Профессиональный взлом имеет следующую структуру (восстановите последовательность)

1) попытка внедрения вредоносных программ

2) поиск уязвимостей в ПО ЗИ

3) тщательный анализ ПО

4) анализ выбранной политики безопасности

12. Когда пользователь знает что-то, что подтверждает его подлинность, то существуют следующие способы аутентификации:

1) парольная аутентификация

2) аутентификация по магнитному носителю

3) модель рукопожатия

4) аутентификация по характеристикам работы пользователя

13. Когда пользователь что-то имеет, что подтверждает его подлинность, то существуют следующие способы аутентификации:

1) парольная аутентификация

2) аутентификация по магнитному носителю

3) модель рукопожатия

4) аутентификация по характеристикам работы пользователя

14. К защите от удаленного НСД можно отнести:

1) модель рукопожатия

2) Протокол Kerberos

3) Аутентификация по биометрическим характеристикам

4) Аутентификация по росписи мышью

15. Целью защиты информации является:

1) предотвращение хищения, утечки, искажения, утраты и подделки информации;

2) предотвращение несанкционированных действий по уничтожению, модификации, копированию и блокированию информации;

3) реализация права на государственную тайну и конфиденциальную информацию

4) выявление правил и норм поведения человека, направленные на обеспечение безопасности информации

16. К основным видам средств защиты информации относится:

1) нормативно-правовые

2) Технические

3) Экологические

4) Этнические

17. Технические средства защиты – это

1) правила, меры и мероприятия, регламентирующие вопросы доступа, хранения, применения и передачи информации

2) это комплексы специального технического и программного обеспечения

3) правила и нормы поведения, направленные на обеспечение безопасности информации

4) законы и другие правовые акты, а также механизмы их реализации, регламентирующие информационные отношения в обществе

18. К каналам утечки информации относится:

1) Магнитный канал

2) Виброакустический канал

3) Лазерный канал

4) Специальный канал

19. К назначению ОС относится:

1)управление процессором путем чередования выполнения программ;

2)обработка прерываний и синхронизация доступа к ресурсам вычислительной системы;

3)управление памятью путем выделения программам на время их выполнения требуемой памяти;

4)поддержка работы всех программ, обеспечение их взаимодействия с аппаратурой;

20. Многопроцессорная обработка в ОС бывает:

1) Симметричной

2) Квадратичной

3) Полной

4) Ассиметричной

21. К локальной защите от НСД относится:

1) Аутентификация на основе биометрических характеристик

2) Протокол CHAP

3) Парольная аутентификация

4) Проток PAP

22. Когда пользователь и есть то лицо, за которое себя выдает то существуют следующие способы аутентификации:

1) парольная аутентификация

2) аутентификация по магнитному носителю

3) модель рукопожатия

4) аутентификация по характеристикам работы пользователя

23. Какой протокол направленный для защиты от удаленного НСД основан на использовании одноразовых паролей.

1) PAP

2) CHAP

3) S/KEY

4) Kerberos

24. К недостаткам дискреционного управления доступом относится:

1) нельзя контролировать утечку конфиденциальной информации

2) неудобство для пользователя

3) нет опасности утечки конфиденциальной информации

4) слабая защита от вредоносных программ

25. Запись определенных событий в журнал безопасности сервера называется

1) аудитом

2) мониторингом

3) трафиком

4) учетом

Модуль 2. Классификация функциональных требований по защите информации и данных.

1. Защита исполняемых файлов обеспечивается

1) обязательным контролем попытки запуска

2) криптографией

3) специальным режимом запуска

4) дополнительным хостом

2. Защита от форматирования жесткого диска со стороны пользователей обеспечивается

1) аппаратным модулем, устанавливаемым на системную шину ПК

2) системным программным обеспечением
3) специальным программным обеспечением
4) аппаратным модулем, устанавливаемым на контроллер

3. Из перечисленного ACL-список содержит:

1) срок действия маркера доступа;
2) домены, которым разрешен доступ к объекту;
3) операции, которые разрешены с каждым объектом;
4) тип доступа

4. Из перечисленного базовыми услугами для обеспечения безопасности компьютерных систем и сетей являются:

1) аутентификация;
2) идентификация;
3) целостность;
4) контроль доступа;
5) контроль трафика;
6) причастность

5. Из перечисленного в обязанности сотрудников группы информационной безопасности входят:

1) управление доступом пользователей к данным;
2) расследование причин нарушения защиты;
3) исправление ошибок в программном обеспечении;
5) устранение дефектов аппаратной части

6. Из перечисленного в ОС UNIX существуют администраторы:

1) системных утилит;
2) службы контроля;
3) службы аутентификации;
4) тиражирования;
5) печати;
6) аудита

7. Из перечисленного в файловых системах ОС UNIX права доступа к файлу определяются для:

1) владельца;
2) членов группы владельца;
3) конкретных заданных пользователей;
4) конкретных заданных групп пользователей;
5) всех основных пользователей

8. Из перечисленного для аутентификации по отпечаткам пальцев терминальных пользователей используются методы:

1) сравнение отдельных случайно выбранных фрагментов;
2) сравнение характерных деталей в графическом представлении;
3) непосредственное сравнение изображений;
4) сравнение характерных деталей в цифровом виде

9. Из перечисленного для разграничения доступа к файлу применяются флаги, разрешающие:

1) копирование;
2) чтение;
3) запись;
4) выполнение;
5) удаление

10. Из перечисленного доступ к объекту в многоуровневой модели может рассматриваться как:

1) чтение;
2) удаление;
3) копирование;
4) изменение

11. Из перечисленного контроль доступа используется на уровнях:
1) сетевом;
2) транспортном;
3) сеансовом;
4) канальном;
5) прикладном;
6) физическом

12. Из перечисленного методами защиты потока сообщений являются:
1) нумерация сообщений;
2) отметка времени;
3) использование случайных чисел;
4) нумерация блоков сообщений;
5) копирование потока сообщений

13. Из перечисленного на транспортном уровне рекомендуется применение услуг:
1) идентификации;
2) конфиденциальности;
3) контроля трафика;
4) контроля доступа;
5) целостности;
6) аутентификации

14. Из перечисленного подсистема управления криптографическими ключами структурно состоит из:
1) центра распределения ключей;
2) программно-аппаратных средств;
3) подсистемы генерации ключей;
4) подсистемы защиты ключей

15. В чем заключается метод защиты информации - разделение доступа (привилегий)?
1) В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.
2) В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.
3) В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.
4) В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду.
5) В исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

16. В чем заключается метод защиты информации - разграничение доступа?

1) В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.
2) В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.
3) В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.
4) В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду.
5) В исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

17. В чем заключается метод защиты информации - ограничение доступа?
1) В создании некоторой физической замкнутой преграды вокруг объекта защиты с организацией контролируемого доступа лиц, связанных с объектом защиты по своим функциональным обязанностям.
2) В разделении информации, циркулирующей в объекте защиты, на части и организации доступа к ней должностных лиц в соответствии с их функциональными обязанностями и полномочиями.
3) В том, что из числа допущенных к ней должностных лиц выделяется группа, которой предоставляется доступ только при одновременном предъявлении полномочий всех членов группы.
4) В преобразовании информации с помощью специальных алгоритмов либо аппаратных решений и кодов ключей, т.е. в приведении ее к неявному виду.
5) В исполнении существующих в стране или введении новых законов, положений, постановлений и инструкций, регулирующих юридическую ответственность должностных лиц-пользователей и обслуживающего технического персонала за утечку, потерю или модификацию доверенной ему информации, подлежащей защите, в том числе за попытки выполнить аналогичные действия за пределами своих полномочий, а также ответственности посторонних лиц за попытку преднамеренного несанкционированного доступа к аппаратуре и информации.

18. На чем основан принцип работы антивирусных мониторов?
1) На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю.
2) На проверке файлов, секторов и системной памяти и поиске в них известных и новых(неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски.
3) На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т. д.
4) На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные.

19. На чем основан принцип работы антивирусных иммунизаторов?

1) На защите системы от поражения вирусом какого-то определенного вида. Файлы на дисках модифицируются таким образом, что вирус принимает их за уже зараженные.

2) На проверке файлов, секторов и системной памяти и поиске в них известных и новых(неизвестных сканеру) вирусов. Для поиска известных вирусов используются маски.

3) На подсчете контрольных сумм для присутствующих на диске файлов или системных секторов. Эти суммы затем сохраняются в базе данных антивируса, а также другая информация: длина файлов, дата их последней модификации и т. д.

4) На перехватывании вирусоопасных ситуаций и сообщении об этом пользователю.

20. Что необходимо сделать при обнаружении файлового вируса?

1) Компьютер необходимо отключить от сети и проинформировать системного администратора.

2) Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются.

3) Вместо отключения компьютера от сети достаточно на период лечения убедиться втом, что соответствующий редактор неактивен.

21. Что необходимо сделать при обнаружении загрузочного вируса?

1) Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются.

2) Компьютер необходимо отключить от сети и проинформировать системного администратора.

3) Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен.

22. Что необходимо сделать при обнаружении макровируса?

1) Вместо отключения компьютера от сети достаточно на период лечения убедиться в том, что соответствующий редактор неактивен.

2) Компьютер необходимо отключить от сети и проинформировать системного администратора.

3) Компьютер от сети отключать не следует, так как вирусы этого типа по сети не распространяются.

23. В чем заключается принцип работы сетевого вируса?

1) Вирусы используют для своего распространения протоколы или команды компьютерных сетей и электронной почты.

2) Вирусы либо различными способами внедряются в выполняемые файлы, либо создают файлы-двойники, либо используют особенности организации файловой системы;

3) Вирусы записывают себя либо в загрузочный сектор диска, либо в сектор, содержащий системный загрузчик винчестера, либо меняют указатель на активный boot-сектор.

4) Вирусы заражают файлы-документы и электронные таблицы популярных редакторов.

24. Источником каких угроз информации являются санкционированные программно-аппаратные средства?

1) запуск технологических программ, способных при некомпетентном использовании вызывать потерю работоспособности системы (зависания или зацикливания) или необратимые изменения в системе (форматирование или реструктуризацию носителей информации, удаление данных и т.п.); возникновение отказа в работе операционной системы.

2) стихийные бедствия; магнитные бури; радиоактивное излучение.

3) внедрение агентов в число персонала системы; вербовка персонала или отдельных пользователей, имеющих определенные полномочия; угроза несанкционированного копирования секретных данных пользователем; разглашение, передача или утрата атрибутов разграничения доступа.
4) нелегальное внедрение и использование неучтенных программ (игровых, обучающих, технологических и др., не являющихся необходимыми для выполнения нарушителем своих служебных обязанностей) с последующим необоснованным расходованием ресурсов (загрузка процессора, захват оперативной памяти и памяти на внешних носителях); заражение компьютера вирусами с деструктивными функциями.

25. Какие угрозы информации относятся к искусственным?
1.) ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков; структурные, алгоритмические и программные ошибки; действия человека, направленные на несанкционированные воздействия на информацию.
2) отказы и сбои аппаратуры; помехи на линиях связи от воздействий внешней среды; аварийные ситуации; стихийные бедствия.
3) аварийные ситуации; стихийные бедствия; ошибки человека как звена системы; схемные и системотехнические ошибки разработчиков.

Модуль 3. Программно-аппаратные средства защиты информации

1. Под угрозой безопасности информации в компьютерной системе (КС)понимают:
A. возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации;
B. событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации;
C. действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.
2. Уязвимость информации — это:
A. возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации;
B. событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации;
C. это действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.
3. Атакой на КС называют:
A. возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации;
B. событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации;
C. действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.
4. Искусственные угрозы исходя из их мотивов разделяются на:
A. непреднамеренные и преднамеренные;
B. косвенные и непосредственные;
C. несанкционированные и санкцианированные.
5. К непреднамеренным угрозам относятся:

A. ошибки в разработке программных средств КС;

B. несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями;

C. угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой.

6. К умышленным угрозам относятся:

A. несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС);

B. воздействие на аппаратные средства КС физических полей других электронных устройств (при несоблюдении условий их электромагнитной совместимости) и др.

C. ошибки пользователей КС.

7. Косвенными каналами утечки называют:

A. каналы, не связанные с физическим доступом к элементам КС;

B. каналы, связанные с физическим доступом к элементам КС;

C. каналы, связанные с изменение элементов КС и ее структуры.

8. К косвенным каналам утечки информации относятся:

A. использование подслушивающих (радиозакладных) устройств;

B. маскировка под других пользователей путем похищения их идентифицирующей информации (паролей, карт и т.п.);

C. злоумышленное изменение программ для выполнения ими несанкционированного копирования информации при ее обработке.

9. Непосредственными каналами утечки называют:

A. каналы, связанные с физическим доступом к элементам КС;

B. каналы, не связанные с физическим доступом к элементам КС;

C. каналы, связанные с изменение элементов КС и ее структуры.

10. К непосредственным каналам утески информации относятся:

A. обход средств разграничения доступа к информационным ресурсам вследствие недостатков в их программном обеспечении и др.

B. перехват побочных электромагнитных излучений и наводок(ПЭМИН);

C. дистанционное видеонаблюдение.

11. Избирательная политика безопасности подразумевает, что:

A. права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности);

B. все субъекты и объекты системы должны быть однозначно идентифицированы;

C. каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации.

12. Полномочная политика безопасности подразумевает, что:

A. каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ;

B. все субъекты и объекты системы должны быть идентифицированы;

C. права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности).

13. Достоверная вычислительная база – это:

A. абстрактное понятие, обозначающее полностью защищенный механизм вычислительной системы (включая аппаратные и программные средства), отвечающий за поддержку реализации политики безопасности;

B. активный компонент системы, который может явиться причиной потока информации от объекта к объекту или изменения состояния системы;

C. пассивный компонент системы, хранящий, принимающий или передающий информацию.

14. Достоверная вычислительная база выполняет задачи:

A. поддерживает реализацию политики безопасности и является гарантом целостности механизмов защиты;

B. функционирует на фоне избирательной политики, придавая ее требованиям иерархически упорядоченный характер (в соответствии с уровнями безопасности);

C. представляет собой некоторый набор требований, прошедших соответствующую проверку, реализуемых при помощи организационных мер.

15. Идентификация объекта – это:

A. одна из функций подсистемы защиты;

B. взаимное установление подлинности объектов, связывающихся между собой по линиям связи;

C. сфера действий пользователя и доступные ему ресурсы КС.

16. Процедуру установки сфер действия пользователя и доступные ему ресурсы КС называют:

A. авторизацией;

B. аутентификацией;

C. идентификацией.

17. Авторизация – это:

A. предоставление полномочий;

B. подтверждение подлинности;

C. цифровая подпись.

18. Аутентификация – это:

A. подтверждение подлинности;

B. предоставление полномочий;

C. цифровая подпись.

19. Для проведения процедур идентификации и аутентификации пользователя необходимо:

A. наличие соответствующего субъекта (модуля) аутентификации;

B. наличие аутентифицирующего объекта, хранящего уникальную информацию;

C. ответы a) и b).

20. Биометрическая идентификация и аутентификация пользователя это:

A. идентификация потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения;

B. схема идентификации, позволяющая увеличить число аккредитаций, выполняемых за один цикл, и, тем самым уменьшить длительность процесса идентификации;

C. схема идентификации с нулевой передачей знаний.

21. Для чего используется процедура “рукопожатия”:

A. для взаимной проверки подлинности;

B. для распределения ключей между подлинными партнерами;

C. для безопасного использования интеллектуальных карт.

22. Параллельная схема идентификации позволяет увеличить:

A. число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации;

B. регистрацию времени для каждого сообщения;

C. объект-эталон для идентификации и аутентификации пользователей.

23. Какие существуют формы представления объектов, аутентифицирующих пользователя:

A. внешний аутентифицирующий объект, не принадлежащий системе;

B. внутренний объект, принадлежащий системе, в который переносится информация из внешнего объекта;
C. варианты a) и b).

24. Внешняя и внутренняя формы представления аутентифицирующего объекта должны быть:
A. семантически тождественны;
B. модифицированы;
C. структурированы.

25. Внешние объекты могут быть технически реализованы на различных носителях информации?
A. да;
B. нет;
C. не знаю.

Модуль 4. Программно-аппаратные средства защиты информации при передаче по каналам связи.

1. Для чего создается система разграничения доступа к информации:
A. для защиты информации от НСД;
B. для осуществления НСДИ;
C. определения максимального уровня конфиденциальности документа.

2. Сбои, отказы технических и программных средств могут быть использованы для НСД?
A. да;
B. нет;
C. не знаю.

3. Какие методы организации разграничения доступа используются в КС:
A. матричный;
B. структурированный;
C. метод Гиллоу-Куискуотера.

4. Мандатный метод основывается на:
A. многоуровневой модели защиты;
B. использование матриц доступа;
C. криптографическом преобразовании.

5. Какой из функциональных блоков должна содержать система разграничения доступа к информации:
A. блок криптографического преобразования информации при ее хранении и передаче;
B. блок контроля среды размещения;
C. блок контроля среды выполнения.

6. Диспетчер доступа реализуется в виде:
A. аппаратно-программных механизмов;
B. аппаратных механизмов;
C. программных механизмов.

7. Под ядром безопасности понимают:
A. локализованную, минимизированную, четко ограниченную и надежно изолированную совокупность программно-аппаратных механизмов, доказательно правильно реализующих функции диспетчера доступа;
B. сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления;
C. событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации.

8. Главным условием создания ядра безопасности является:
   A. обеспечение многоуровневого режима выполнения команд;
   B. мандатное управление;
   C. матричная структура.
9. Под организацией доступа к ресурсам понимается
   A. весь комплекс мер, который выполняется в процессе эксплуатации КС для предотвращения несанкционированного воздействия на технические и программные средства, а также на информацию;
   B. хранения атрибутов системы защиты, поддержки криптографического закрытия информации, обработки сбоев и отказов и некоторые другие;
   C. предотвращение несанкционированного перехода пользовательских процессов в привилегированное состояние.
10. При эксплуатации механизмов аутентификации основными задачами являются:
   A. генерация или изготовление идентификаторов, их учет и хранение, передача идентификаторов пользователю и контроль над правильностью выполнения процедур аутентификации в КС;
   B. разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц;
   C. реализация механизма виртуальной памяти с разделением
   D. адресных пространств.
11. В чем заключается правило разграничения доступа
   A. лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа;
   B. лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа;
   C. лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, не содержатся все категории, определенные для данного документа.
12. Правильность функционирования ядра безопасности доказывается путем:
   A. полной формальной верификации его программ и пошаговым доказательством их соответствия выбранной математической модели защиты;
   B. использования дополнительных программных или аппаратно-программных средств;
   C. использования строго определенного множества программ.
13. Мандатное управление позволяет упростить процесс регулирования доступа?
   A. да;
   B. нет;
   C. не знаю.
14. Матричное управление доступом предполагает использование:
   A. матриц доступа;
   B. аппаратно-программных механизмов;
   C. субъекта допуска.
15. Основной проблемой создания высокоэффективной защиты от НСД является
   A. предотвращение несанкционированного перехода пользовательских процессов в привилегированное состояние;

B. использования дополнительных программных или аппаратно-программных средств;

C. разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц.

16. Выберите правильную характеристику позиционной системы кодирования экономической информации

A. Отражает порядковые номера кодируемой номенклатуры.
B. Отражает иерархическую соподчиненность классификационных признаков
C. Отражает номера серий кодируемой номенклатуры.
D. Отражает мнемонику кодируемой номенклатуры.

17. С какой целью осуществляется кодирование информации

A. Сокращение трудовых затрат при вводе информации.
B. Упрощение вычислительных операций.
C. Упрощение процедур сортировки данных.
D. Удобства процедур оформления управленческих документов.
E. Упрощение процедур передачи данных.

18. Укажите функции электронного документооборота

A. Решение прикладных задач.
B. Хранение электронных документов в архиве.
C. Поиск электронных документов в архиве.
D. Организация решения транзакционных задач.
E. Маршрутизация и передача документов в структурные подразделения.
F. Мониторинг выполнения распоряжений.
G. Организация решения аналитических задач.

19. Укажите распространенные формы внутримашинного представления структурированных информационных ресурсов

A. Базы данных.
B. Традиционные бумажные управленческие документы.
C. Базы знаний.
D. Тексты приказов, введенные в компьютер.
E. Хранилища данных.
F. Web-сайты.

20. Укажите главную особенность баз данных

A. Ориентация на передачу данных.
B. Ориентация на оперативную обработку данных и работу с конечным пользователем.
C. Ориентация на интеллектуальную обработку данных.
D. Ориентация на предоставление аналитической информации.

21. Укажите главную особенность хранилищ данных

A. Ориентация на оперативную обработку данных.
B. Ориентация на аналитическую обработку данных.
C. Ориентация на интерактивную обработку данных.
D. Ориентация на интегрированную обработку данных.

22. Укажите понятия, характеризующие реляционную модель базы данных

A. Имя таблицы (отношения).
B. Файл.
C. Атрибут.
D. Кортеж.
E. Вектор.
F. Матрица.
G. Домен.

23. С какой целью создаются системы управления базами данных
   A. Создания и обработки баз данных.
   B. Обеспечения целостности данных.
   C. Кодирования данных.
   D. Передачи данных.
   E. Архивации данных
24. Централизованная база данных характеризуется
   A. Оптимальным размером.
   B. Минимальными затратами на корректировку данных.
   C. Максимальными затратами на передачу данных.
   D. Рациональной структурой.
25. Распределенная база данных характеризуется
   A. Оптимальным размером.
   B. Минимальными затратами на передачу данных.
   C. Максимальными затратами на корректировку данных.
   D. Иерархической структурой.
   E. Конфиденциальностью данных.

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста (25 вопросов в варианте)	Неправильный ответ / Правильный ответ	0,4

Лабораторные работы

Цель проведения лабораторных работы – практическое освоение материала дисциплины.

Темы лабораторных работ

Модуль 1. Основные принципы программно-аппаратных средств обеспечения информационной безопасности.

1) Средства разграничения доступа.
2) Использование встроенных в операционную систему Windows средств разграничения доступа.
3) Использование встроенных в операционную систему Linux средств разграничения доступа.
4) Особенности использования мандатного метода разграничения доступа.

Модуль 2. Классификация функциональных требований по защите информации и данных.

5) Доверенная загрузка ПК.
6) Использование средств антивирусной защиты.
7) Система аудита операционных систем.
8) Средства резервного копирования данных.
9) Программно–аппаратные комплексы, применяемые для резервного копирования.

Модуль 3. Программно-аппаратные средства защиты информации

10) Установка и настройка СЗИ Dallas Lock 8.0.
11) Настройка СЗИ Dallas Lock 8.0.
12) Особенности использования СЗИ Dallas Lock 8.0 К.
13) Особенности использования СЗИ Dallas Lock 8.0 С.

Модуль 4. Программно-аппаратные средства защиты информации при передаче по каналам связи.

14) Применение электронных замков.
15) Использование программы шифрования дисков True Crypt.
16) Смарт карты.
17) Биометрические системы аутентификации.

Лабораторная работа № 1

Модуль 2. Классификация функциональных требований по защите информации и данных.

Тема: Использование средств антивирусной защиты..

Цель: ознакомиться с теоретическими аспектами защиты информации от вредоносных программ: разновидностями вирусов, способами заражения и методы борьбы. Ознакомиться с различными видами программных средств защиты от вирусов. Проверка настроек антивирусов, сканирование файлов, папок и дисков, обновления антивирусной базы. Получить навыки работы с антивирусным пакетом Антивирус Касперского.

Задание: Создать зашифрованный файловый контейнер. Защитить с помощью приложения TrueCrypt флеш-носитель паролем. Создать зашифрованный файловый контейнер.

Порядок выполнения:

1. Изучить антивирусный пакет Антивирус Касперского.
2. Выполнить сканирование папок на наличие вирусов.
3. Произвести обновление антивирусной базы
4. Ответить на контрольные вопросы:
   a) Что называется компьютерным вирусом?
   b) Какая программа называется "зараженной"?
   c) Что происходит, когда зараженная программа начинает работу?
   d) Как может маскироваться вирус?
   e) Каковы признаки заражения вирусом?
   f) Каковы последствия заражения компьютерным вирусом?
   g) По каким признакам классифицируются компьютерные вирусы?
   h) Как классифицируются вирусы по среде обитания?
   i) Какие типы компьютерных вирусов выделяются по способу воздействия?
   j) Что могут заразить вирусы?
   k) Как маскируются "невидимые" вирусы?
   l) Каковы особенности самомодифицирующихся вирусов?
   m) Какие методы защиты от компьютерных вирусов можно использовать?
   n) В каких случаях применяют специализированные программы защиты от компьютерных вирусов?
   o) На какие виды можно подразделить программы защиты от компьютерных вирусов?
   p) Как действуют программы-детекторы?
   q) Что называется сигнатурой?
   r) Всегда ли детектор распознает зараженную программу?
   s) Каков принцип действия программ-ревизоров, программ-фильтров, программ-вакцин?
   t) Как выглядит многоуровневая защита от компьютерных вирусов с помощью антивирусных программ?
   u) Перечислите меры защиты информации от компьютерных вирусов.
   v) Каковы современные технологии антивирусной защиты?

w) Каковы возможности антивируса Касперского для защиты файловых серверов и почтовых серверов?
x) Какие модули входят всостав антивируса Касперского для защиты файловых систем?
y) Каково назначение этих модулей?
z) Какие элементы электронного письма подвергаются проверке на наличие вирусов?
aa) Как обезвреживаются антивирусом Касперского обнаруженные подозрительные или инфицированные объекты?
bb) Как обновляется база вирусных сигнатур?

5. Защита лабораторной работы. Проводится в форме устного опроса после выполнения работы.

Критерии оценки лабораторной работы

Структура работы	Критерии оценки	Распределение баллов
Одно лабораторное задание Модуль 1 Модуль 2 Модуль 3 Модуль 4	работа выполнена с ошибками и не получены ответы на все контрольные вопросы/ работа выполнена, но не получены ответы на все контрольные вопросы/ работа выполнена и получены ответы на все контрольные вопросы	 0/2/4 0/2/5 0/2/4 0/1/3

Практические работы

Цель проведения практических работ – практическое освоение материала дисциплины.

Темы практических работ

Модуль 1. Основные принципы программно-аппаратных средств обеспечения информационной безопасности.

1. Анализ угроз информационной безопасности..
2. Классификация ПАСОИБ.
3. Методы разграничения доступа.
4. Особенности мандатного метода разграничения доступа.

Модуль 2. Классификация функциональных требований по защите информации и данных.

5. Журналы регистрации событий на примере ОС Windows.
6. Пожарная система сигнализации.
7. Охранная система сигнализации.
8. Системы сигнализации на примере гуманитарного корпуса БашГУ.
9. Система контроля и управления доступом (СКУД) на примере гуманитарного корпуса БашГУ.

Модуль 3. Программно-аппаратные средства защиты информации

10. Программно-аппаратные средства защиты от несанкционированного доступа к информации, хранимой в ПЭВМ.
11. Электронные замки.
12. Смарт карты.
13. Штатные средства сетевого оборудования, предназначенные для защиты информации при передаче по каналам связи.

Модуль 4. Программно-аппаратные средства защиты информации при передаче по каналам связи.

14. Методы криптографической защиты.
15. Применение симметричных алгоритмов шифрования.
16. Применение ассиметричных алгоритмов шифрования.
17. Использование электронной подписи.

Практическая работа №5
Модуль 2. Классификация функциональных требований по защите информации и данных.
Тема: Журналы регистрации событий на примере ОС Windows.
Цель: Практическое ознакомление с системой журналирования, применяемой в ОС Windows.
Задание: Ознакомиться с системой журналирования ОС Windows.
Порядок выполнения:
1) Ознакомиться с системой журналирования ОС Windows.
2) Показать ключевые журналы ОС Windows.
3) Указать типичные проблемы, возникающие при обработке указанных журналов.
4) Перечислить типовые пути решения возникающих проблем.

Критерии оценки практической работы

Структура работы	Критерии оценки	Распределение баллов
Одно практическое задание Модуль 1 Модуль 2 Модуль 3 Модуль 4	работа выполнена с ошибками и не получены ответы на все контрольные вопросы/ работа выполнена, но не получены ответы на все контрольные вопросы/ работа выполнена и получены ответы на все контрольные вопросы	 0/2/4 0/2/5 0/2/4 0/1/3

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. Информационные технологии : учебник / Ю.Ю. Громов, И.В. Дидрих, О.Г. Иванова, Долозов, Н.Л. Программные средства защиты информации : конспект лекций / Н.Л. Долозов, Т.А. Гультяева ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2015. - 63 с. : схем., ил. - Библиогр. в кн. - ISBN 978-5-7782-2753-8; То же [Электронный ресурс]. - URL:http://biblioclub.ru/index.php?page=book&id=438307

2. Программно-аппаратные средства обеспечения информационной безопасности: учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, К.В. Славнов, Е.В. Кравцов ; под ред. А.В. Душкина. - Москва : Горячая линия - Телеком, 2016. - 248 с. : схем., табл., ил. - Библиогр.: с. 234-235 - ISBN 978-5-9912-0470-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=483768.

Дополнительная литература

3. Волкова, Т.В. Основы проектирования компонентов автоматизированных систем : учебное пособие [Электронный ресурс]/ / Т.В. Волкова ; Министерство образования и науки Российской Федерации, Оренбургский Государственный Университет, Кафедра

программного обеспечения вычислительной техники и автоматизированных систем. - Оренбург : ОГУ, 2016. - 226 с. Режим доступа - URL: http://biblioclub.ru/index.php?page=book&id=471129.

4. Гухман, В.Б. Краткая история науки, техники и информатики : учебное пособие [Электронный ресурс]/ В.Б. Гухман. - Москва ; Берлин : Директ-Медиа, 2017. - 171с. [Электронный ресурс]/ URL: http://biblioclub.ru/index.php?page=book&id=474295.

5. Синицын, Ю.И. Сети и системы передачи информации : учебное пособие[Электронный ресурс]/ Ю.И. Синицын, Е. Ряполова, Р.Р. Галимов ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего образования «Оренбургский государственный университет». - Оренбург : ОГУ, 2017. - 190 с. – Режим доступа : http://biblioclub.ru/index.php?page=book&id=485524.

6. Губарев, В.В. Введение в теоретическую информатику : учебное пособие / В.В. Губарев ; Министерство образования и науки Российской Федерации, Новосибирский государственный технический университет. - Новосибирск : НГТУ, 2014. - Ч. 1. - 420 с. : табл., граф., схем., ил. - Библиогр.: с. 452-457. - ISBN 978-5-7782-2477-3; То же [Электронный ресурс]. - URL:http://biblioclub.ru/index.php?page=book&id=436214

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 «ЭБ БашГУ» https://elib.bashedu.ru
3. Электронная библиотечная система БашГУ – www.bashlib.ru
4. Электронная библиотечная система издательства «Лань» https://e.lanbook.com
5. Антиплагиат.ВУЗ. Договор № 81 от 27.04.2018 г. Срок действия лицензии до 04.05.2019 г., договор № 1104 от 18.04.2019 г. Срок действия лицензии до 04.05.2020 г
6. Банк нормативно-правовых актов РФ Министерства юстиции РФ http://zakon.scli.ru/ru/legal_texts/index.php
7. Справочная правовая система Консультант Плюс. Договор №31705775411 от 07.12.2017 г. http://www.consultant-plus.ru
8. Национальные стандарты РФ в области информационной безопасности: http://www.iso27000.ru/standarty/gost-r-nacionalnye-standarty-rossiiskoi-federacii-v-oblasti-zaschity-informacii
9. Нормативные документы и материалы сайта ФСТЭК России (Федеральной службы по техническому и экспортному контролю России): https://fstec.ru/ Раздел «Национальные старты информационной безопасности» (https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/113-gosudarstvennye-standarty/377-gosudarstvennye-standarty)

Государственные информационно-правовые системы:

1. Научный центр правовой информации при министерстве Юстиций РФ http://www.scli.ru
2. Официальный интернет-портал правовой информации http://pravo.gov.ru
3. Информационно-правовая система «Законодательство России» http://pravo.fso.gov.ru
4. Модуль «Документы Президент России» http://www.kremlin.ru/acts
5. Банк документов, подписанных Президентом России http://kremlin.ru/acts/bank
6. База данных «Федеральные законы» http://graph.garant.ru:8080/SESSION/PILOT/main.htm
7. Автоматизированная система обеспечения законодательной деятельности государственной думы (законопроекты и законодательные инициативы)

http://asozd.duma.gov.ru/

8. База данных «Издания по общественным и гуманитарным наукам» (на платформе East View) Ссылка http://www.ebiblioteka.ru (вход из сети вуза без регистрации).
9. Банк данных "Библиотека копий официальных публикаций правовых актов» при ассоциации юристов России http://alrf.consultant.ru/
10. Банк данных "Копии правовых актов: Российская Федерация» http://giod.consultant.ru/
11. Банк данных "Нормативно-правовые акты Федерального Собрания Российской Федерации http://duma.consultant.ru/

Другие профессиональные базы данных и информационно-справочные системы:

1. Электронная база данных диссертаций РГБ (авторизованный доступ по паролю в сети вуза) – Ссылка: http://dvs.rsl.ru
2. База данных «Вестники Московского университета» (на платформе East View) (вход без регистрации). Ссылка http://www.ebiblioteka.ru/browse/udb/12.
3. Annual Reviews – обзор журналов по общественно-научной тематике и др. – доступ из сети вуза. – Ссылка: http://www.annualreviews.org/
4. Computers & Applied Sciences Complete (EBSCO) доступ в сети вуза, язык английский. Ссылка: http://search.ebscohost.com/
5. SCOPUS наукометрическая, библиографическая и реферативная база данных издательской корпорации Elsevier. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://www.scopus.com/
6. Taylor and Francis – База полнотекстовых научных журналов, книг. Язык английский. – доступ из сети вуза. – Ссылка: http://www.tandf
7. Web of Science наукометрическая, библиографическая и реферативная база данных издательской корпорации Thomson Reuters. Язык английский, вход после регистрации или из сети вуза. – Ссылка: http://apps.webofknowledge.com/
8. Wiley Полнотекстовая база данных статей из 1400 журналов издательства Wiley по всем отраслям знаний. Язык английский. Доступ из сети вуза без регистрации. – Ссылка: http://onlinelibrary.wiley.com/
9. Сайт по информационной безопасности: http://securitypolicy.ru/; его раздел: «Документы, стандарты и методики по информационной безопасности»: http://securitypolicy.ru/
10. Докипедия: http://dokipedia.ru
11. Словари и энциклопедии On-Linehttp://www.dic.academic.ru

Программное обеспечение

1. 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.
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.

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

Наименование специальных помещений и помещений для самостоятельной работы	Вид Занятия	Оснащенность специальных помещений и помещений для самостоятельной работы
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 (гуманитарный корпус). **2.** ***учебная аудитория для проведения лабораторных работ:*** компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **3.** ***учебная аудитория для проведения групповых и индивидуальных консультаций:*** 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 № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус),	Лекции, практические занятия, самостоятельные работы, групповые и индивидуальные опросы	**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. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт APAPT MA1225 – 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 APAPT MA1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор

компьютерный класс аудитория № 420 (гуманитарный корпус). **4.** ***учебная аудитория для текущего контроля и промежуточной аттестации:*** 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 № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **5.** ***помещения для самостоятельной работы:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **6.** ***помещение для хранения и профилактического обслуживания учебного оборудования:***аудитория № 523 (гуманитарный корпус).		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 № 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. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки

		стационарные 15 шт. **Компьютерный класс аудитория № 404** 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.

Приложение № 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Программно-аппаратная защита информации** на 5 семестр
___очная_ф/о___

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	2 ЗЕТ / 72 часа
Учебных часов на контактную работу с преподавателем:	54,2
лекций	18
практических/ семинарских	18
лабораторных	18
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на самостоятельную работу обучающихся (СР)	17,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на подготовку к зачету (Контроль)	–

Форма контроля
Зачет 5 семестр

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Программно-аппаратная защита информации** на 6 семестр
___очная_ф/о___

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	5 ЗЕТ / 180 часов
Учебных часов на контактную работу с преподавателем:	51,2
лекций	16
практических/ семинарских	16
лабораторных	16
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	3,2
из них, предусмотренные на выполнение курсовой работы / курсового проекта	_
Учебных часов на самостоятельную работу обучающихся (СР)	102
из них, предусмотренные на выполнение курсовой работы / курсового проекта	_
Учебных часов на подготовку к экзамену (Контроль)	27

Форма контроля
Экзамен 2 семестр

Семестр 5

№	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	8	9
1	Модуль 1. Основные принципы программно-аппаратных средств обеспечения информационной безопасности. Тема: Основные понятия и определения в области создания программно–аппаратных средств обеспечения информационной безопасности. Тема: Анализ угроз информационной безопасности. Тема: Нормативно-правовая база создания программно–аппаратных средств обеспечения информационной безопасности. Тема: Классификация ПАСОИБ. Тема: Основные этапы проектирования программно–аппаратных средств обеспечения информационной безопасности.	2 2 2 2 2	2 2 2 2 2	2 2 2 2 2	2 2 2 2 2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	практическая работа, лабораторная работа, тест
2	Модуль 2. Классификация функциональных требований по защите информации и данных. Тема: Принципы действия и технологические особенности программно-аппаратных средств,	2	2	2	2	Самостоятельное изучение рекомендуемой основной и	практическая работа, лабораторная работа, тест

	реализующих отдельные функциональные требования по защите информации и данных и их взаимодействие с общесистемными компонентами вычислительных систем.					дополнительной литературы	
	Тема: Методы обеспечения идентификации и аутентификации.	2	2	2	2		
	Тема: Методы криптографической защиты.	2	2	2	2		
	Тема: Методы и средства ограничения доступа к компонентам вычислительных систем.	2	2	2	1,8		
Всего часов		18	18	18	17,8		

Семестр 6

№	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	8	9
1	Модуль 3. Программно-аппаратные средства защиты информации. Тема: Классификация аппаратных компонентов средств защиты программ. Тема: Классификация программных компонентов средств защиты программ. Тема: Способы защиты программ от незаконного использования. Способы изучения кода программ. Тема: Изолированная программная среда.	 2 2 2 2	 2 2 2 2	 4 4	 13 13 13 13	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	практическая работа, лабораторная работа, тест
2	Модуль 4. Программно-аппаратные средства защиты информации при передаче по каналам связи. Тема: Основные принципы разграничения доступа к сетевым ресурсам. Тема: Программно-аппаратные средства обнаружения сетевых атак. Тема: Программно-аппаратные средства управления безопасностью сети. Тема: Проверка объекта информатизации на базе вычислительной техники.	 2 2 2 2	 2 2 2 2	 4 2 2	 13 13 13 11,2	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	практическая работа, лабораторная работа, тест

	16	16	16	102,2	
Всего часов	34	34	34	120	