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
Организационная защита информации

Обязательная часть (Б1.О.20)

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-5 Способен планировать проведение работ по комплексной защите информации на объекте информатизации.	ОПК-5.1 Знает методы, этапы, принципы постановки задач при планировании проведения работ по комплексной защите информации на объекте информатизации.	Знать методы, этапы, принципы постановки задач при планировании проведения работ по комплексной защите информации на объекте информатизации.
		ОПК-5.2 Умеет осуществлять планирование проведения работ по комплексной защите информации на объекте информатизации.	Уметь осуществлять планирование проведения работ по комплексной защите информации на объекте информатизации.

		ОПК-5.3 Владеет методами планирования проведения работ по комплексной защите информации на объекте информатизации.	Владеть методами планирования проведения работ по комплексной защите информации на объекте информатизации.
Эксплуатационные	ОПК-8 Способен реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	ОПК-8.1 Знает основные принципы и методы реализации комплекса мер по обеспечению безопасности информации, обеспечения комплексной защиты информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	Знать основные принципы и методы реализации комплекса мер по обеспечению безопасности информации, обеспечения комплексной защиты информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.
		ОПК-8.2 Умеет реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	Уметь реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.
		ОПК-8.3 Владеет принципами и методами реализации комплекса мер по обеспечению безопасности информации, обеспечению комплексной защиты	Владеть программными средствами принципами и методами реализации комплекса мер по обеспечению безопасности информации, обеспечению комплексной защиты

		информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Организационная защита информации» относится к обязательной части.

Дисциплина изучается на 2 курсе в 4 семестре.

Целью учебной дисциплины «Организационная защита информации», является формирование навыков планирования и реализации работ по обеспечению безопасности и комплексной защиты информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.

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	Уметь осуществлять критический анализ проблемных ситуаций на основе системного	Не умеет.	Умеет осуществлять критический анализ проблемных ситуаций на основе

на основе системного подхода, вырабатывать стратегию действий.	подхода, вырабатывать стратегию действий.		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.

ОПК-5. Способен планировать проведение работ по комплексной защите информации на объекте информатизации.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ОПК-5.1 Знает методы, этапы, принципы постановки задач при планировании проведения работ по комплексной защите информации на объекте информатизации.	Знать методы, этапы, принципы постановки задач при планировании проведения работ по комплексной защите информации на объекте информатизации.	Не знает или показывает очень слабые знания.	Знает методы, этапы, принципы постановки задач при планировании проведения работ по комплексной защите информации на объекте информатизации.
ОПК-5.2 Умеет осуществлять планирование проведения работ по комплексной защите информации на объекте информатизации.	Уметь осуществлять планирование проведения работ по комплексной защите информации на объекте информатизации.	Не умеет.	Умеет осуществлять планирование проведения работ по комплексной защите информации на объекте информатизации.
ОПК-5.3 Владеет методами планирования проведения работ по комплексной защите информации на объекте информатизации.	Владеть методами планирования проведения работ по комплексной защите информации на объекте информатизации.	Не владеет.	Владеет методами планирования проведения работ по комплексной защите информации на объекте информатизации.

ОПК-8. Способен реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ОПК-8.1 Знает основные принципы и методы реализации комплекса мер по обеспечению безопасности информации, обеспечения комплексной защиты информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	Знать основные принципы и методы реализации комплекса мер по обеспечению безопасности информации, обеспечения комплексной защиты информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	Не знает или показывает очень слабые знания.	Знает основные принципы и методы реализации комплекса мер по обеспечению безопасности информации, обеспечения комплексной защиты информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.
ОПК-8.2 Умеет реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	Уметь реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	Не умеет.	Умеет реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.
ОПК-8.3 Владеет принципами и методами реализации комплекса мер по обеспечению безопасности информации, обеспечению комплексной защиты информации и	Владеть принципами и методами реализации комплекса мер по обеспечению безопасности информации, обеспечению комплексной защиты информации и сведений,	Не владеет.	Владеет принципами и методами реализации комплекса мер по обеспечению безопасности информации, обеспечению комплексной защиты информации и

сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.		сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.

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
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
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

ОПК-5. Способен планировать проведение работ по комплексной защите информации на объекте информатизации.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ОПК-5.1 Знает методы, этапы, принципы постановки задач при планировании проведения работ по комплексной защите информации на объекте информатизации.	Знать методы, этапы, принципы постановки задач при планировании проведения работ по комплексной защите информации на объекте информатизации.	тестирование, практическое задание
ОПК-5.2 Умеет осуществлять планирование проведения работ по комплексной защите информации на объекте информатизации.	Уметь осуществлять планирование проведения работ по комплексной защите информации на объекте информатизации.	тестирование, практическое задание
ОПК-5.3 Владеет методами планирования проведения работ по комплексной защите информации на объекте информатизации.	Владеть методами планирования проведения работ по комплексной защите информации на объекте информатизации.	тестирование, практическое задание

ОПК-8. Способен реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ОПК-8.1 Знает основные принципы и методы реализации комплекса мер по обеспечению безопасности информации, обеспечения комплексной защиты информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	Знать основные принципы и методы реализации комплекса мер по обеспечению безопасности информации, обеспечения комплексной защиты информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	тестирование, практическое задание
ОПК-8.2 Умеет реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать	Уметь реализовывать комплекс мер по обеспечению безопасности информации, обеспечивать комплексную защиту информации и сведений,	тестирование, практическое задание

комплексную защиту информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	
ОПК-8.3 Владеет принципами и методами реализации комплекса мер по обеспечению безопасности информации, обеспечению комплексной защиты информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	Владеть принципами и методами реализации комплекса мер по обеспечению безопасности информации, обеспечению комплексной защиты информации и сведений, составляющих государственную тайну, на объекте информатизации с учетом решаемых задач и структуры объекта информатизации, внешних воздействий и вероятных угроз.	тестирование, практическое задание

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 зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

(для зачета:

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

не зачтено – от 0 до 59 рейтинговых баллов).

Рейтинг – план дисциплины
«Организационная защита информации»

Специальность: 10.05.05 Безопасность информационных технологий в правоохранительной сфере

курс 2, семестр 4

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Организационное обеспечение информационной безопасности.				
Текущий контроль				
Практическая работа	5	8	0	40
Рубежный контроль				

Тест	10	1	0	10
Всего			0	50
Модуль 2. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах.				
Текущий контроль				
Практическая работа	5	8	0	40
Рубежный контроль				
Тест	10	1	0	10
Всего			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

Зачет

Вопросы для зачета:

1. Понятие «организационная защита информации».
2. Организация охраны территории.
3. Организация охраны зданий.
4. Организация охраны помещений.
5. Организация охраны персонала.
6. Организационные источники и каналы утечки.
7. Силы, средства и условия организационной защиты информации.
8. Особенности системы организационной защиты информации, составляющей государственную тайну.
9. Особенности системы организационной защиты информации, составляющей коммерческую тайну.
10. Организация подготовки и проведения совещаний и переговоров по конфиденциальным вопросам.
11. Порядок засекречивания конфиденциальных сведений, документов и изделий.
12. Порядок рассекречивания конфиденциальных сведений, документов и изделий.
13. Организация защиты информации при приеме в организации посетителей и командированных лиц.
14. Подбор персонала на должности, связанные с работой с конфиденциальнойинформацией.
15. Организация защиты информации при осуществлении рекламной и публикаторской деятельности.
16. Допуск к секретной информации.
17. Организация защиты информации при подготовке материалов к открытомуопубликованию.

18. Организация доступа к конфиденциальной информации.
19. Аналитическая работа как основа управления системой организационной защитыинформации.
20. Текущая работа с персоналом, обладающим конфиденциальной информацией.
21. Планирование процессов организационной защиты информации.
22. Организация служебного расследования по фактам разглашения персоналомконфиденциальной информации.
23. Контроль функционирования системы организационной защиты информации.
24. Организация охраны территории, зданий, помещений и персонала.
25. Требования к помещениям и хранилищам, в которых ведутся закрытые работы ихранятся конфиденциальные документы и изделия.
26. Типовые организационные структуры государственной системы защиты информации.
27. Функции контроля и надзора органа государственной власти в области обеспечения безопасности и защиты информации.
28. Специфика государственного регулирования деятельности специализированных предприятий — разработчиков комплексов и средств обеспечения безопасности.
29. Классификация услуг организационно-технологического характера в соответствии с этапами жизненного цикла систем обеспечения информационной безопасности.
30. Специфика деятельности сертификационно-испытательных центров (лабораторий) и механизмов ее государственного регулирования.
31. Какие функции выполняет служба безопасности предприятия для решения задачи физической защиты.
32. Функции служба безопасности предприятия для решения задачи обеспечения информационной безопасности.
33. Структура полномасштабной системы обеспечения безопасности и защиты информации.
34. Специфика организации и выполнения охранных функций.
35. Специальные мероприятия и действия сотрудников службы безопасности по организации объектовых режимов.
36. Основное назначение корпоративной нормативной базы службы безопасности .
37. Структура корпоративной нормативной базы службы безопасности.
38. Разделы типового формата положений о структурных подразделениях службы безопасности.
39. Перечень и краткая характеристика основных нормативных документов процедурного уровня ИБ.
40. Чем определяется срок жизненного цикла корпоративной нормативной базы по информационной безопасности.
41. Различие в определениях политики информационной безопасности.
42. Отличие нормативно-методических документов политики безопасности от нормативных документов процедурного уровня.
43. Особенности документального оформления политики безопасности, и чем они объясняются.
44. Типовое содержание политики безопасности, оформленной в виде единого документа.
45. Назначение Концепции обеспечения информационной безопасности организации.
46. Содержание Концепции обеспечения информационной безопасности организации.

47. Цель и задача аудита информационной безопасности.
48. Методология деятельности по обеспечению безопасности объекта на основе политики безопасности.
49. Перечень контрольных мероприятий и действий по оценке уровня безопасности объекта.
50. Определение понятия «режимный объект» и видов обеспечения его безопасности.
51. Цель и задачи организации пропускного режима.
52. Нормативная основа организации пропускного режима и каково ее общее содержание.
53. Порядок пропуска (прохода) физических лиц на территорию режимного объекта.
54. Правила въезда (выезда) транспортных средств на территорию режимного объекта.
55. Особенности организации охраны режимного объекта.

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).

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. Организационное обеспечение информационной безопасности.

1. Выберите правильный ответ
Основным источником права в области обеспечения информационной безопасности в России является
а) Уголовный кодекс
б) Конституция
в) государственные и отраслевые стандарты
г) Документы Гостехкомиссии
2. Выберите правильный ответ
В статье 42 Конституции РФ говорится о том, что
а) каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, на тайну переписки, телефонных переговоров, почтовых, телеграфных и иных сообщений

б) сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускаются

в) каждый имеет право свободно искать, получать, передавать, производить и распространять информацию любым законным способом, перечень сведений, составляющих государственную тайну, определяется федеральным законом

г) каждый имеет право на достоверную информацию о состоянии окружающей среды

3. Дополните предложение

Федеральные законы и другие нормативные акты предусматривают разделение информации на категории свободного и ___**ограниченного**___ доступа.

4. Выберите правильный ответ

В соответствии с Указом Президента Российской Федерации № 212 от 19.02.99 г., межотраслевую координацию и функциональное регулирование деятельности по обеспечению защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную и служебную тайну, осуществляет коллегиальный орган

а) ФАПСИ

б) ФСБ

в) Гостехкомиссия

г) Головная научно-исследовательская организация по защите информации

5. Выберите правильный ответ

Совокупность норм гражданского права, регулирующих отношения по признанию авторства и охране имущественных и неимущественных прав авторов и правообладателей - это определение

а) сертификата

б) авторского права

в) патента

г) товарного знака

6. Дополните предложение

Авторские права на все виды программ для ЭВМ (в том числе на операционные системы и программные комплексы), которые могут быть выражены на любом языке и в любой форме, включая исходный текст и объектный код, охраняются так же, как авторские права на произведения_**литературы**_.

7. Выберите правильный ответ

Правообладатель для оповещения о своих правах может, начиная с первого выпуска в свет программы для ЭВМ или базы данных, использовать знак охраны авторского права

а) ©

б) ®

в) ™

г) ∀

8. Выберите правильный ответ

Символ ® означает

а) патент

б) охраняемый знак

в) торговую марку

г) авторское право

9. Выберите правильный ответ

Программы для ЭВМ и базы данных к объектам авторского права

а) относятся

б) относятся в исключительных случаях

в) не относятся

10. Дополните предложение

Основной принцип компьютерной стеганографии предполагает использование двух типов файлов – файл-**_сообщение_**, которое должно быть скрыто, и файл-контейнер.

11. Выберите правильный ответ

Согласно статьи 24 Конституции РФ сбор, хранение, использование и распространение информации о частной жизни лица без его согласия

а) возможны в исключительных случаях

б) проводится постоянно

в) не допускается

12. Выберите правильный ответ

Каждый имеет право на достоверную информацию о состоянии окружающей среды это выдержка из следующей статьи Конституции РФ

а) 23

б) 24

в) 29

г) 42

13. Дополните предложение

Государственная тайна относится к информации **_ограниченного_** доступа

14. Выберите правильный ответ

Комплекс действий, проводимых с целью подтверждения соответствия определенным нормам ГОСТ и других нормативных документов называется

а) лицензированием

б) сертификацией

в) авторским правом

г) торговой маркой

15. Выберите правильный ответ

Способ оформления уникальных идей - это определение

а) сертификата

б) авторского права

в) патента

г) товарного знака

16. Дополните предложение

Авторское право действует с момента создания программы для ЭВМ или базы данных в течение всей жизни автора и **_50_** лет после его смерти.

17. Выберите правильный ответ

Символ © означает

а) патент

б) охраняемый знак

в) торговую марку

г) авторское право

18. Выберите правильный ответ

Символ ™ означает

а) патент

б) охраняемый знак

в) торговую марку

г) авторское право

19. Выберите правильные ответы

Незаконное использование программ для ЭВМ либо иное нарушение авторских прав на программы для ЭВМ влечет за собой

а) гражданско-правовую ответственность

б) административную

в) уголовную

20. Дополните предложение

Компьютерная стеганография относится к методам, предусматривающие __**наличие**_ скрытой авторской «подписи», внедряемой в цифровой файл, как правило, с использованием стеганографических технологий.

21. В автоматизированной системе класса **3Б** работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности, обрабатывается «Служебная тайна».

22. Ущерб от реализации риска может быть - и _ **материальный и нематериальный**_

23. При внедрении организационных мер защиты информации осуществляются: введение _**ограничений**_ на действия персонала (пользователей (операторского персонала), администраторов, обеспечивающего персонала), а также на условия эксплуатации, изменение состава и конфигурации и _**технических средств и программного обеспечения**_, а также _ **реализация**_ правил разграничения доступа, регламентирующих права доступа субъектов доступа к объектам доступа.

24. Какие существуют основные уровни обеспечения защиты информации?

а) Законодательный

б) Организационно-административный

в) Программно-технический (аппаратный)

г) Физический

д) Вероятностный

е) Распределительный

25. Какие основные свойства информации и систем обработки информации необходимо поддерживать, обеспечивая информационную безопасность?

а) Доступность

б) Целостность

в) Конфиденциальность

г) Управляемость

д) Сложность

Модуль 2. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах.

1 Что такое политика информационной безопасности

а) Методология защиты информации

б) Идеология информационной безопасности

в) Концепция защиты информации

2 Какой федеральный закон считается рамочным по защите информации?

а) ФЗ «О коммерческой тайне»

б) ФЗ «О персональных данных»

в) ФЗ «Об информации, информационных технологиях и о защите информации»

3 Номер ФЗ «Об информации, информационных технологиях и о защите информации» является:

а)188 ФЗ

б)152 ФЗ

в)149 ФЗ

г)214 ФЗ

4 Лицензирование деятельности по распространению криптографических средств, осуществляет:

а) ФСБ

б) ФСТЭК

в) Роскомнадзор

г) Ростехнадзор

5 Подключение ИС, обрабатывающих служебную тайну к сети Интернет:

а) допускается

б) не допускается

в) допускается только с использованием специально предназначенных для этого средств

г) допускается только с использованием средств защиты известных производителей

6 Специальная проверка это

а) выявление возможных каналов утечки информации Российскими техническими средствами

б) определение соответствия условий эксплуатации ОИ требованиям аттестатов соответствия объектам защиты

в) проверки технических средств на наличие возможно внедренных электронных устройств перехвата информации

7 Каким документов определяются права человека на доступ к информации?

а) Доктриной ИБ

б) Конституцией

в) ФЗ «О коммерческой тайне»

8 В соответствии с каким Гостом производится аттестация объекта информатизации?

а) ГОСТ РО 0043-004-2013

б) ГОСТ ISO 17799

в) BS 7799

9 Источниками угроз несанкционированного доступа являются: (выберите все верные варианты ответов)

а) нарушители

б) природные факторы

в) носители вредоносных программ

г) аппаратные закладки

д) отказы оборудования

е) отказы программного обеспечения

10 Основные направления обеспечения информационной безопасности указанные в Доктрине ИБ

а) стратегическое развитие военных конфликтов, которые могут возникнуть в результате применения информационных технологий;

б) совершенствование Вооруженных Сил Российской Федерации

в) прогнозирование, обнаружение и оценка информационных угроз, включая угрозы Вооруженным Силам Российской Федерации в информационной сфере

г) содействие обеспечению защиты интересов союзников Российской Федерации в информационной сфере.

11. Техническими каналами утечки информации, приводящими к возникновению угроз безопасности персональных данных являются:

(выберите все верные варианты ответов)

а) кражи технических средств информационной системы

б) утечки акустической (речевой) информации

в) утечки информации реализуемые через общедоступные информационные сети

г) утечки видовой информации

д) утечки информации по каналам побочных электромагнитных излучений

е) утечки информации реализуемые через интернет

12. Документом, определяющим лицензируемые виды деятельности, является:

а) Постановление правительства РФ от 26 января 2006 г. № 45 Об организации лицензирования отдельных видов деятельности

б) Постановление Правительство РФ от 15 августа 2006 г. № 504 О лицензировании деятельности по технической защите конфиденциальной информации

в) Постановление Правительства РФ от 31 августа 2006 г. № 532 О лицензировании деятельности по разработке и (или) производству средств защиты конфиденциальной информации

г) ФЗ «О лицензировании отдельных видов деятельности» 99-ФЗ от 4 мая 2011 г.

д) ФЗ «О техническом регулировании» 184-ФЗ от 27 декабря 2002 г.

13. Средствами защиты информации, подлежащими сертификации являются: (выберите все верные варианты ответов)

а) строительные материалы, используемые для отделки помещений в которых размещаются отдельные элементы ИСПДн

б) детали интерьера, используемые для размещения ИСПДн

в) средства контроля эффективности применения средств защиты информации

г) средства контроля эффективности прочности ограждений

д) средства защиты информации (технические, программные, программно-технические) от НСД, блокировки доступа и нарушения целостности

14. Основными направлениями обеспечения информационной безопасности в области государственной и общественной безопасности являются:

а) противодействие использованию информационных технологий для пропаганды экстремистской идеологии, распространения ксенофобии, идей национальной исключительности в целях подрыва суверенитета, политической и социальной стабильности, насильственного изменения конституционного строя, нарушения территориальной целостности Российской Федерации

б) осуществление контроля за населением РФ с использованием технических средств и информационных технологий специальными службами и организациями иностранных государств, а также отдельными лицами

в) повышение защищенности критической информационной инфраструктуры и устойчивости ее функционирования, развитие механизмов обнаружения и предупреждения информационных угроз и ликвидации последствий их проявления, повышение защищенности граждан и территорий от последствий чрезвычайных ситуаций, вызванных информационно-техническим воздействием на объекты критической информационной инфраструктуры

г) допущения иностранного контроля за функционированием объектов информатизации, на территории Российской Федерации

15. Перечислить нормативно-методические документы по анализу угроз и уязвимостей

а) BS 7799-3

б) ISO 27005

в) BSI IT Baseline Protection Manual

г) ГОСТ 3328

16. «Информационная система» это:

а) совокупность информации, информационных технологий и технических средств

б) совокупность информации, информационных технологий, технических средств и персонала, обслуживающего систему

в) совокупность информационных технологий и технических средств

г) совокупность информации, технических средств и персонала, обслуживающего информационную систему

д) совокупность информации, технических средств и персонала, обслуживающего и эксплуатирующего информационную систему

17. Количество категорий внутренних нарушителей для ИСПДн, определяемых нормативными документами ФСТЭК:

а) 4

б) 5

в) 6

г) 7
д) 8
е) 9

18. Классами защищённости автоматизированных систем от несанкционированного доступа являются: (выберите все верные варианты ответов)

а) 1Е
б) 2Г
в) 2А
г) 2В
д) 3С
е) 3Б

19. Основными элементами ИС являются:
(выберите все верные варианты ответов)

а) помещения для размещения технических средств
б) персональные данные, содержащиеся в базах данных
в) контролируемая зона
г) информационные технологии
д) обслуживающий персонал
е) технические средства обработки информации
ж) ограждающие конструкции
з) технические средства перевозки материальных носителей информации

20. Каким нормативными документами регламентируется деятельность по выявлению угроз

а) BS 7799
б) ISO 27005
в) BSI IT Baseline Protection Manual
г) ГОСТ 3328
д) Приказ ФСТЭК № 31

21. К методам и способам защиты информации в информационных системах относятся методы и способы защиты информации от _**несанкционированного доступа**_ и методы и способы защиты информации от _**утечки по техническим каналам**_

22. Классификация угроз информационной безопасности, по виду активов делиться на угрозы, направленные против _**информационных активов**_ и угрозы, направленные против _**технических средств**_

23. Основные требования к системе защиты автоматизированной системы управления должны содержать - _**класс защищенности**_ автоматизированной системы управления, перечень _**нормативных правовых актов**_, локальных правовых актов, _**методических документов**_, национальных стандартов и стандартов организаций, которым должна _**соответствовать**_ автоматизированная система управления и объекты защиты автоматизированной системы управления на каждом из ее уровней

24. При проектировании системы защиты автоматизированной системы управления необходимо: определять типы _**субъектов доступа (пользователи, процессы и иные субъекты доступа**_ и _**объектов доступа**_, являющихся объектами защиты (автоматизированные рабочие места, промышленные серверы, телекоммуникационное оборудование, программируемые логические контроллеры, исполнительные устройства, иные объекты доступа), определять _**методы управления доступом**_ (дискреционный, мандатный, ролевой), типы _**доступа**_ (чтение, запись, выполнение) и правила _**разграничения**_ доступа субъектов доступа к объектам доступа (на основе списков, меток безопасности, ролей и иных правил), подлежащие реализации в автоматизированной системе управления, выбирать меры защиты информации, подлежащие реализации в рамках системы защиты автоматизированной системы управления

25. Разрабатывать организационно-распорядительные документы по защите информации, определяющие правила и процедуры (политики) включает в себя
реализацию отдельных мер защиты информации в автоматизированной системе управления в рамках ее **_системы защиты_** и **_планирования мероприятий_** по обеспечению защиты информации в автоматизированной системе управления

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста (25 вопросов в варианте) Модуль 1 Модуль 2	Неправильный ответ / Правильный ответ	 0,4 0,4

Практические работы

Цель проведения практических работ – практическое освоение материала дисциплины.

Темы практических работ

Модуль 1. Организационное обеспечение информационной безопасности.
1. Анализ законодательных актов в области организации защиты информации
2. Методы контроля ресурсов.
3. Создание системы обеспечения информационной безопасности предприятия.
4. Принципы классификации ресурсов.
5. Классификация источников информации ограниченного доступа на предприятии.
6. Виды проверок СУИБ.
7. Разработка нормативных документов организации на основе стандарта ГОСТ Р ИСО/МЭК 27037-2014 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Руководства по идентификации, сбору, получению и хранению свидетельств, представленных в цифровой форме».
8. Ответственность за информационные ресурсы.
Модуль 2. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах.
9. Организация работ с информацией, составляющей служебную тайну.
10. Разработка плана мероприятий по обеспечению засекречивания и рассекречивания информации.
11. Изучение основных принципов допускной работы.
12. Составление перечня внутренних организационно-распорядительных документов по защите информации на объекте.
13. Порядок назначения комиссии для аттестации помещений на пригодность их для ведения закрытых работ.
14. Определение состава информации, используемой в ходе совещания или переговоров.
15. Разработка должностных инструкций пользователей АС с учетом требований информационной безопасности.
16. Проблемы построения современных систем безопасности.

Практическая работа № 2
Модуль 1. Системы управления ИБ.
Тема: Методы контроля ресурсов.
Цель: Практическое ознакомление с методами контроля ресурсов.
Задание: На практике ознакомиться с методами контроля ресурсов.

Порядок выполнения:

1. Ознакомиться с разделом 7.2 ГОСТ Р ИСО/МЭК 27002-2012 Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности и ГОСТ Р 58545-2019 Менеджмент знаний. Руководящие указания по сбору, классификации, маркировке и обработке информации.
2. Ознакомиться с набором процедур маркировки и обработки информации.
3. Приведите примеры маркировки информации.
4. Ответить на контрольные вопросы:

a) Какие требования предъявляются к маркировке информации?
b) Информация представленная в какой форме подвергается процедуре маркировки?
c) Для каких классов информации необходима маркировка?
d) Какие требования предъявляются к классификации информации?
e) На что направлена процедура маркировки информации?
f) Дайте определение терминов «ICMH-система», «информационные активы», «маркировка», «материальные носители информации», «жизненный цикл информации».

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

Критерии оценки практической работы

Структура работы	Критерии оценки	Распределение баллов
Одно практическое задание Модуль 1 Модуль 2	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	 0/2/5 0/2/5

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. Сергеева, Ю.С. Защита информации: Конспект лекций : учебное пособие / Ю.С. Сергеева. - Москва : А-Приор, 2011. - 128 с. - (Конспект лекций). - ISBN 978-5-384-00397-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=72670

2. Петренко, В.И. Защита персональных данных в информационных системах : учебное пособие / В.И. Петренко ; Министерство образования и науки Российской Федерации, Федеральное государственное автономное образовательное учреждение высшего профессионального образования «Северо-Кавказский федеральный университет». - Ставрополь : СКФУ, 2016. - 201 с. : схем. ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=459205

Дополнительная литература

3. Основы информационной безопасности : учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. - Москва : Горячая линия - Телеком, 2011.

- 558 с. : ил. - ISBN 5-93517-292-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253056

4. Системы защиты информации в ведущих зарубежных странах : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов, Г.В. Кондрашин, М.В. Рудановский. - 4-е изд., стер. - Москва : Издательство «Флинта», 2016. - 224 с. - (Организация и технология защиты информации). - Библиогр.: с. 192-193 - ISBN 978-5-9765-1274-0 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93351

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-Line- http://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 специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения
1	2	3
1. ***учебная аудитория для проведения занятий лекционного типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). ***2. учебная аудитория для проведения занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). ***3. учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус),	Лекции, практические работы	**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 АРАРТ МА1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516**

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). ***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:***аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).		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 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.

Приложение № 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Организационная защита информации** на 4 семестр
___очная_ф/о___

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	2 ЗЕТ / 72 часа
Учебных часов на контактную работу с преподавателем:	48,2
лекций	16
практических/ семинарских	32
лабораторных	–
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)	23,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на подготовку к зачету (Контроль)	–

Форма контроля
Зачет 4 семестр

Семестр 4

№	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. Организационное обеспечение информационной безопасности. Тема: Основные понятия в области организационной защиты информации. Тема: Работа с персоналом, обладающим конфиденциальной информацией. Тема: Организация служебного расследования по фактам разглашения персоналом конфиденциальной информации. Тема: Технические средства обеспечения информационной безопасности.	2 2 2 2	4 4 4 4		3 3 3 3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	практическая работа, тест
2	Модуль 2. Общесистемные основы защиты информации и процесса ее обработки в вычислительных системах Тема: Организационные источники и каналы утечки информации. Тема: Подбор персонала на должности, связанные с работой с конфиденциальной информацией. Тема: Организация охраны территории, зданий,	2 2 2	4 4 4		3 3 3	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	практическая работа, тест

	помещений и персонала. Тема: Силы, средства и условия организационной защиты информации.	2	4		2,8		
Всего часов		16	32	0	23,8		