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
Информационная безопасность в правоохранительной сфере

Обязательная часть (Б1.О.11)

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**
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.
Аналитические	ОПК-10 Способен осуществлять аналитическую деятельность с последующим использованием данных при решении профессиональных задач.	ОПК-10.1 Знает направления, этапы и методы аналитической деятельности с последующим использованием данных при решении профессиональных задач.	Знать направления, этапы и методы аналитической деятельности с последующим использованием данных при решении профессиональных задач.
		ОПК-10.2 Умеет использовать аналитическую деятельность с последующим использованием данных при решении профессиональных задач.	Уметь использовать аналитическую деятельность с последующим использованием данных при решении профессиональных задач.
		ОПК-10.3 Владеет методами осуществления аналитической деятельности с последующим использованием данных при решении профессиональных задач.	Владеть методами осуществления аналитической деятельности с последующим использованием данных при решении профессиональных задач.

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность в правоохранительной сфере» относится к обязательной части.

Дисциплина изучается на 4 курсе в 7,8 семестрах.

Целью учебной дисциплины «Информационная безопасность в правоохранительной сфере», является формирование навыков планирования и проведения работ по комплексной защите информации в автоматизированных системах и проведения аналитической деятельности с последующим использованием данных при обеспечении информационной безопасности в автоматизированных системах.

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.

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			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
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 основные методы, этапы, принципы постановки задач при планировании проведения работ по комплексной защите информации на объекте информатизации, но допускае	Знает основные методы, этапы, принципы постановки задач при планировании проведения работ по комплексной защите информации на объекте информатизации.	Знает методы, этапы, принципы постановки задач при планировании проведения работ по комплексной защите информации на объекте информатизации.

			т ошибки при их применении.		
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 основных работ по комплексной защите информации на объекте информатизации, но при этом допускает ошибки.	Умеет осуществлять планирование проведения основных работ по комплексной защите информации на объекте информатизации.	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 основными методами планирования проведения работ по комплексной защите информации на объекте информатизации, но при этом допускает ошибки.	Владеет основными методами планирования проведения работ по комплексной защите информации на объекте информатизации.	Владеет методами планирования проведения 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	Знать методы, этапы, принципы постановки задач при планировании	Не знает или показывает очень слабые знания.	Знает методы, этапы, принципы постановки задач при

задач при планировании проведения работ по комплексной защите информации на объекте информатизации.	проведения работ по комплексной защите информации на объекте информатизации.		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-10. Способен осуществлять аналитическую деятельность с последующим использованием данных при решении 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-10.1 Знает направления, этапы и методы аналитической деятельности с последующим использованием данных при решении профессиональных задач.	Знать направления, этапы и методы аналитической деятельности с последующим использованием данных при решении профессиональных задач.	Не знает или показывает очень слабые знания.	Знает основные направления, этапы и методы аналитической деятельности с последующим использованием данных при решении профессиональных задач, но делает ошибки при их выборе.	Знает основные направления, этапы и методы аналитической деятельности с последующим использованием данных при решении профессиональных задач.	Знает направления, этапы и методы аналитической деятельности с последующим использованием данных при решении профессиональных задач.
ОПК-10.2	Уметь использовать	Не умеет.	Умеет	Умеет	Умеет

Умеет использовать аналитическую деятельность с последующим использованием данных при решении профессиональных задач.	аналитическую деятельность с последующим использованием данных при решении профессиональных задач.		использовать основные методы аналитической деятельности с последующим использованием данных при решении профессиональных задач, но делает ошибки при их использовании.	использовать основные методы аналитической деятельности с последующим использованием данных при решении профессиональных задач.	использовать аналитическую деятельность с последующим использованием данных при решении профессиональных задач.
ОПК-10.3 Владеет методами осуществления аналитической деятельности с последующим использованием данных при решении профессиональных задач.	Владеть методами осуществления аналитической деятельности с последующим использованием данных при решении профессиональных задач.	Не владеет.	Владеет основными методами осуществления аналитической деятельности с последующим использованием данных при решении профессиональных задач, но делает ошибки при их использовании.	Владеет основными методами осуществления аналитической деятельности с последующим использованием данных при решении профессиональных задач.	Владеет методами осуществления аналитической деятельности с последующим использованием данных при решении профессиональных задач.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		Не зачтено	Зачтено
ОПК-10.1 Знает направления, этапы и методы	Знать направления, этапы и методы аналитической	Не знает или показывает очень слабые знания.	Знает направления, этапы и методы аналитической

аналитической деятельности с последующим использованием данных при решении профессиональных задач.	деятельности с последующим использованием данных при решении профессиональных задач.		деятельности с последующим использованием данных при решении профессиональных задач.
ОПК-10.2 Умеет использовать аналитическую деятельность с последующим использованием данных при решении профессиональных задач.	Уметь использовать аналитическую деятельность с последующим использованием данных при решении профессиональных задач.	Не умеет.	Умеет использовать аналитическую деятельность с последующим использованием данных при решении профессиональных задач.
ОПК-10.3 Владеет методами осуществления аналитической деятельности с последующим использованием данных при решении профессиональных задач.	Владеть методами осуществления аналитической деятельности с последующим использованием данных при решении профессиональных задач.	Не владеет.	Владеет методами осуществления аналитической деятельности с последующим использованием данных при решении 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

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; лабораторная работа
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; лабораторная работа
ОПК-5.3 Владеет методами планирования проведения работ по комплексной защите	Владеть методами планирования проведения работ по комплексной защите информации на объекте	тестирование, практическое задание; лабораторная работа

информации на объекте информатизации.	информатизации.	

ОПК-10. Способен осуществлять аналитическую деятельность с последующим использованием данных при решении профессиональных задач.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ОПК-10.1 Знает направления, этапы и методы аналитической деятельности с последующим использованием данных при решении профессиональных задач.	Знать направления, этапы и методы аналитической деятельности с последующим использованием данных при решении профессиональных задач.	тестирование, практическое задание; лабораторная работа
ОПК-10.2 Умеет использовать аналитическую деятельность с последующим использованием данных при решении профессиональных задач.	Уметь использовать аналитическую деятельность с последующим использованием данных при решении профессиональных задач.	тестирование, практическое задание; лабораторная работа
ОПК-10.3 Владеет методами осуществления аналитической деятельности с последующим использованием данных при решении профессиональных задач.	Владеть методами осуществления аналитической деятельности с последующим использованием данных при решении 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
«Информационная безопасность в правоохранительной сфере»

курс 4, семестр 7

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Защита государственной и коммерческой тайны в системе защиты информации.				

Текущий контроль			0	
Практическая работа	6	5	0	30
Рубежный контроль				
Тест	20	1	0	20
Всего			0	50
Модуль 2. Государственная тайна				
Текущий контроль				
Практическая работа	7	4	0	28
Рубежный контроль				
Тест	22	1	0	22
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 4, семестр 8

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 3. Нормативные правовые акты в области информационной безопасности				
Текущий контроль				
Практическая работа	8	4	0	32
Рубежный контроль				
Тест	8	1	0	8
Всего			0	40
Модуль 4. Информационная безопасность в правоохранительных органах				
Текущий контроль				
Практическая работа	6	4	0	24
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. Понятие и защита государственной и коммерческой тайны в системе защиты информации. Принципы защиты защита государственной и коммерческой тайны.
2. Отнесение сведений к коммерческой, служебной и профессиональной тайнам.
3. Правовой режим информационных ресурсов.
4. Признаки охраноспособности информации.
5. Цели защиты информации.
6. Режим защиты информации.
7. Виды защищаемой информации.
8. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
9. Общедоступная информация.
10. Ограничение доступа к информации.
11. Конфиденциальная информация.
12. Виды тайн в российском законодательстве.
13. Персональные данные.
14. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных».
15. Защита коммерческой тайны.
16. Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне».
17. Юридические меры защиты коммерческой тайны.
18. Административно-организационные меры защиты коммерческой тайны.
19. Социально-психологические меры защиты коммерческой тайны.
20. Технические средства защиты коммерческой тайны.
21. Служебная тайна.
22. Признаки профессиональной тайны.
23. Тайна в юридической практике.
24. Тайна в сфере экономической деятельности.
25. Тайна, связанная с этическими соображениями.
26. Государственная тайна и порядок отнесения к ней информации.
27. Закон РФ от 21.7.93 г. № 5485-1 «О государственной тайне»
28. Засекречивание сведений, составляющих государственную тайну.
29. Рассекречивание сведений, составляющих государственную тайну
30. Допуск к государственной тайне.
31. Защита государственной тайны.
32. Организация режима секретности, его особенности и содержание.
33. Организационные и технические способы защиты государственной тайны.
34. Основные нормативные правовые акты в области информационной безопасности и защиты информации.
35. Отечественные и зарубежные стандарты в области информационной безопасности.
36. ГОСТ Р 50922-2006 — Защита информации. Основные термины и определения.
37. Р 50.1.053-2005 — Информационные технологии. Основные термины и определения в области технической защиты информации.
38. ГОСТ Р 51188—98 — Защита информации. Испытание программных средств на

наличие компьютерных вирусов. Типовое руководство.

39. ГОСТ Р 51275-2006 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
40. ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
41. ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности.
42. ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
43. ГОСТ Р ИСО/МЭК 15408 — «Общие критерии оценки безопасности информационных технологий» — стандарт, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; он содержит перечень требований, по которым можно сравнивать результаты независимых оценок безопасности — благодаря чему потребитель принимает решение о безопасности продуктов. Сфера приложения «Общих критериев» — защита информации от несанкционированного доступа, модификации или утечки, и другие способы защиты, реализуемые аппаратными и программными средствами.
44. ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью». Прямое применение международного стандарта с дополнением — ISO/IEC 17799:2005.
45. ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта — ISO/IEC 27001:2005.
46. ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты.
47. РД СВТ. Защита от НСД. Показатели защищенности от НСД к информации — содержит описание показателей защищенности информационных систем и требования к классам защищенности (Проверено 26 июля 2017).
48. Нормативные документы ИБ
49. Стандарт Банка России СТО БР ИББС-1.0-2014 — Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
50. PCI DSS (Payment Card Industry Data Security Standard) — Стандарт безопасности данных индустрии платёжных карт.

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 материалы первого, второго, третьего и четвертого модулей.

Экзаменационные материалы

1. Понятие и защита государственной и коммерческой тайны в системе защиты информации. Принципы защиты защита государственной и коммерческой тайны.
2. Отнесение сведений к коммерческой, служебной и профессиональной тайнам.
3. Правовой режим информационных ресурсов.
4. Признаки охраноспособности информации.
5. Цели защиты информации.
6. Режим защиты информации.
7. Виды защищаемой информации.
8. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации».
9. Общедоступная информация.
10. Ограничение доступа к информации.
11. Конфиденциальная информация.
12. Виды тайн в российском законодательстве.
13. Персональные данные.
14. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных».
15. Защита коммерческой тайны.
16. Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне».
17. Юридические меры защиты коммерческой тайны.
18. Административно-организационные меры защиты коммерческой тайны.
19. Социально-психологические меры защиты коммерческой тайны.
20. Технические средства защиты коммерческой тайны.
21. Служебная тайна.
22. Признаки профессиональной тайны.
23. Тайна в юридической практике.
24. Тайна в сфере экономической деятельности.
25. Тайна, связанная с этическими соображениями.
26. Государственная тайна и порядок отнесения к ней информации.
27. Закон РФ от 21.7.93 г. № 5485-1 «О государственной тайне»
28. Засекречивание сведений, составляющих государственную тайну.
29. Рассекречивание сведений, составляющих государственную тайну
30. Допуск к государственной тайне.
31. Защита государственной тайны.
32. Организация режима секретности, его особенности и содержание.
33. Организационные и технические способы защиты государственной тайны.
34. Основные нормативные правовые акты в области информационной безопасности и защиты информации.
35. Отечественные и зарубежные стандарты в области информационной безопасности.
36. ГОСТ Р 50922-2006 — Защита информации. Основные термины и определения.
37. Р 50.1.053-2005 — Информационные технологии. Основные термины и определения в области технической защиты информации.
38. ГОСТ Р 51188—98 — Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство.
39. ГОСТ Р 51275-2006 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.
40. ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель.
41. ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности

информационных технологий. Часть 2. Функциональные требования безопасности.

42. ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности.
43. ГОСТ Р ИСО/МЭК 15408 — «Общие критерии оценки безопасности информационных технологий» — стандарт, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; он содержит перечень требований, по которым можно сравнивать результаты независимых оценок безопасности — благодаря чему потребитель принимает решение о безопасности продуктов. Сфера приложения «Общих критериев» — защита информации от несанкционированного доступа, модификации или утечки, и другие способы защиты, реализуемые аппаратными и программными средствами.
44. ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью». Прямое применение международного стандарта с дополнением — ISO/IEC 17799:2005.
45. ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования». Прямое применение международного стандарта — ISO/IEC 27001:2005.
46. ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты.
47. РД СВТ. Защита от НСД. Показатели защищенности от НСД к информации — содержит описание показателей защищенности информационных систем и требования к классам защищенности (Проверено 26 июля 2017).
48. Нормативные документы ИБ
49. Стандарт Банка России СТО БР ИББС-1.0-2014 — Стандарт Банка России: «Обеспечение информационной безопасности организаций банковской системы Российской Федерации. Общие положения».
50. PCI DSS (Payment Card Industry Data Security Standard) — Стандарт безопасности данных индустрии платёжных карт.
51. Доктрина информационной безопасности Российской Федерации.
52. Единая система информационно-аналитического обеспечения деятельности МВД России.
53. Основные задачи обеспечения информационной безопасности в правоохранительных органах.
54. Угрозы по добыванию, обработке и использованию оперативно-розыскной информации.
55. Виды категорируемых объектов информации в правоохранительных органах.
56. Специальная проверка.
57. Специальное исследование объекта защиты информации.
58. Специальное обследование.
59. Вопросы безопасности, связанные с персоналом.
60. Соглашения о конфиденциальности.
61. Особенности работы с персоналом, владеющим конфиденциальной информацией.
62. Подбор и подготовка кадров.
63. Проверка персонала на благонадежность.
64. Принципы построения разрешительной системы доступа.
65. Доступ к отчуждаемым носителям конфиденциальной информации.
66. Доступ к средствам вычислительной техники, обрабатывающей конфиденциальную информацию.
67. Текущая работа с персоналом, владеющим конфиденциальной информацией.
68. Служебное расследование.
69. Особенности увольнения сотрудников, владеющих конфиденциальной

информацией.
70. Одностороннее соглашение о неразглашении.
71. Взаимное соглашение о неразглашении.
72. Распространенные недостатки соглашений о неразглашении.
73. Организация противодействия компьютерной преступности.
74. Виды компьютерной преступности в сфере вычислительных сетей.
75. Способы совершения компьютерных преступлений.
76. Ответственность за компьютерные преступления.
77. Методика раскрытия и расследования компьютерных преступлений.
78. Типичные следственные ситуации первоначального этапа и следственные действия в расследовании компьютерных преступлений.
79. Поиск и изъятие информации и следов воздействия на нее в ЭВМ и ее устройствах.
80. Использование специальных познаний и назначение экспертиз.
81. Понятие информационной безопасности. Термины и определения.
82. Система информационной безопасности.
83. Проверка безопасности информационных систем. Аудит систем.
84. Общие сведения об информационной безопасности.
85. Проверка безопасности информационных систем. Мониторинг систем.
86. Основные составляющие информационной безопасности.
87. Внешний аудит.
88. Обоснование необходимости рассмотрения вопросов информационной безопасности.
89. Внутренний аудит.
90. Процессный подход в рамках управления ИБ.
91. Проблемы построения современных систем безопасности.
92. Слежение за доступом к системам и их использованием.
93. Стандарты информационной безопасности ISO/IEC серии 27000.
94. Отраслевые стандарты информационной безопасности
95. Стандарты и нормативные акты РФ в области информационной безопасности.
96. Оценка рисков нарушения безопасности.
97. Средства управления информационной безопасностью.
98. Защита от вредоносного программного обеспечения.
99. Ключевые средства контроля информационной безопасности.
100. Ответственность за информационные ресурсы.
101. Требование бизнеса по обеспечению контроля доступа.
102. Факторы, необходимые для успешной реализации системы информационной безопасности в организации.
103. Управление доступом пользователей. Обязанности пользователей.
104. Группы требований к информационной безопасности организации.
105. Система планирования бесперебойной работы организации.
106. Политика информационной безопасности.
107. Классификация информации.
108. Инфраструктура информационной безопасности.
109. Безопасность информации в должностных инструкциях.
110. Обучение пользователей правилам информационной безопасности.
111. Реагирование на события, таящие угрозу безопасности.
112. Оперирование с носителями информации и их защита.
113. Термины и определения информационной безопасности.
114. Понятие информационной безопасности.
115. Циклическая модель улучшения процессов.

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.

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 Информационная безопасность в правоохранительной сфере

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1. Допуск к государственной тайне.
2. Циклическая модель улучшения процессов.

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

Тестирование

При изучении дисциплины используются тестовые задания закрытого типа. Каждое тестовое задание включает вопрос и не менее 3–х вариантов ответов к нему. Тестирование выполняется в письменной форме.
Необходимо выбрать один или несколько ответов из предложенных вариантов.

Тест № 1
Модуль 1. Защита государственной и коммерческой тайны в системе защиты информации

1. Что не относится к принципам, являющимся основополагающими для правового регулирования отношений, возникающих в сфере информации и ее защиты:

а) системность и последовательность реализации всех этапов правового регулирования;

б) открытость информации о деятельности государственных органов и органов местного самоуправления и свободный доступ к такой информации, кроме случаев, установленных федеральными законами;

в) достоверность информации и своевременность ее предоставления;

г) неприкосновенность частной жизни, недопустимость сбора, хранения, использования и распространения информации о частной жизни лица без его согласия.

2. Виды гражданско-правовых режимов зависимости от характера действий и юридических последствий:

а) конституционный, административный, земельный;

б) собственности, исключительных прав, обязательственного права;

в) материальный, процессуальный;

г) особого регулирования, особой охраны.

3. Что не включается в содержание правового режима информационных ресурсов:

а) порядок документирования информации;

б) положения о доступе к информационным ресурсам в зависимости от их категорий;

в) принятие мер по охране информации (способы охраны и порядок их применения);

г) порядок обеспечения физической защиты граждан, осуществляющих обработку защищаемой информации.

4. Какое понятие является более широким:

а) защита информации;

б) охрана информации;

в) оба понятия равнозначны;

г) эти понятия нельзя сравнивать.

5. Деятельность государственного органа, направленная на восстановление права и пресечение действий, нарушающих право не относится:

а) к неюрисдикционному порядку защиты;

б) к юрисдикционному порядку защиты;

в) к судебному порядку защиты;

г) к административному порядку защиты

6. К правовому режиму информационных ресурсов относится

а) определения объекта права собственности;

б) правила уничтожения субъекта;

в) определение субъекта права собственности или исключительного права;

г) все вышеперечисленное.

7. Какими признаками обладает охраноспособная информация:

а) определен субъект финансирования информационного ресурса;

б) определен порядок доступа к информационному ресурсу;

в) доступ ограничен в соответствии с законом;

г) все перечисленное.

8. Что из указанного относится к понятию «защита информации»:

а) все средства и функции, обеспечивающие доступность, конфиденциальность или целостность информации или связи, исключая средства и функции, предохраняющие от неисправностей. Она включает криптографию, криптоанализ, защиту от собственного излучения и защиту компьютера;

б) деятельность, направленная на предотвращение утечки конфиденциальной информации, несанкционированных и непреднамеренных воздействий на конфиденциальную информацию;

в) комплекс административных, организационных и технических мероприятий по ограничению доступа к информации и ее носителям в целях обеспечения ее сохранности и недоступности третьим сторонам, предусмотренный законодательством РФ;

г) все перечисленное.

9. Защита информации не направлена на:

а) соблюдение конфиденциальности информации ограниченного доступа;

б) нет правильного ответа;

в) реализацию права на доступ к информации;

г) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также иных неправомерных действий в отношении такой информации.

10. К целям защиты информации не относится:

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

б) обеспечение получения выгоды обладателю информации;

в) реализация права на государственную тайну и конфиденциальную информацию;

г) предотвращение несанкционированных действий по уничтожению, модификации, копированию и блокированию информации.

11. Защита информации не осуществляется от:

а) законного требования органа государственной власти об ограничения доступа к информационному ресурсу;

б) утечки (неконтролируемого распространения защищаемой информации в результате ее разглашения, несанкционированного доступа к информации и получения защищаемой информации разведками);

в) разглашения (несанкционированного доведения защищаемой информации до потребителей, не имеющих права доступа к этой информации);

г) разведки (получения защищаемой информации технической, агентурной разведкой).

12. Режим защиты информации устанавливается в отношении:

а) сведений, относящихся к государственной тайне;

б) сведений о стихийных бедствиях, катастрофах и других чрезвычайных событиях, угрожающих безопасности граждан, которые произошли или могут произойти;

в) сведений о неправомерных действиях государственных органов, органов местного и регионального самоуправления и должностных лиц;

г) сведений о состоянии окружающей среды и здоровья населения, его жизненном уровне, в том числе питании, одежде, жилье, медицинском обслуживании и социальном обеспечении, а также о социально- демографических показателях, состоянии правопорядка, образования и культуры населения.

13. Что не относится к конфиденциальной информации:

а) персональные данные;

б) тайна следствия и судопроизводства;

в) государственная тайна;

г) служебная тайна.

14. Какое высказывание не может быть отнесено к общедоступной информации:

а) может использоваться любыми лицами по их усмотрению при соблюдении установленных федеральными законами ограничений в отношении распространения такой информации;

б) обладатель информации, ставшей общедоступной по его решению, не вправе требовать от лиц, распространяющих такую информацию, указывать себя в качестве источника такой информации;

в) информация, размещаемая ее обладателями в сети "Интернет" в формате, допускающем автоматизированную обработку без предварительных изменений человеком в целях повторного ее использования;

г) в случае, если размещение информации в форме открытых данных может привести к распространению сведений, составляющих государственную тайну, размещение указанной информации в форме открытых данных должно быть прекращено по требованию органа, наделенного полномочиями по распоряжению такими сведениями.

15. Укажите правильное полное название Федерального закона:

а) Федеральный закон от 27 июля 2006 г. № 149–ФЗ «Об информации, информационных технологиях и о защите информации»;

б) Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 августа 2006 г. № 149–ФЗ;

в) Федеральный закон от 27 июля 2006 г. № 149–ФЗ «Об информации»;

г) Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27 августа 2007 г. № 149–ФЗ.

16. Основополагающим нормативно-правовым актом в области регулирования персональных данных является:

а) Федеральный закон от 27 июля 2006 г. № 149–ФЗ;

б) Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ;

в) Указ Президента РФ от 6 марта 1997 г. N 188;

г) Закон РФ от 21.07.1993 N 5485-1.

17. В Указе Президента РФ от 6 марта 1997 г. N 188 « Об утверждении перечня сведений конфиденциального характера» не упоминается:

а) общедоступные сведения;

б) все упоминаются;

в) служебная тайна;

г) тайну следствия и судопроизводства.

18. Обеспечение конфиденциальности финансовой информации и защиты коммерческой тайны не реализуется с помощью:

а) технических средств;

б) программно-аппаратными средствами исключительно;

в) мер правовой защиты;

г) социально-психологических инструментов.

19. Не может относиться к категории «служебная тайна»:

а) врачебная тайна;

б) тайна усыновления;

в) коммерческая тайна;

г) нет правильного ответа.

20. В состав процессов “PDCA” входят (по порядку):

а) План, Осуществление, Проверка, Действие

б) Планирование, Реализация, Выполнение, Контроль

в) План, Проверка, Контроль, Выпуск продукции

г) Проникновение, Реализация, Проверка, Действие

21. СОИБ означает:

а) Система обеспечения информационной безопасности

б) Собрание обозначений информационной безопасности

в) Создание объектов инфраструктуры безопасности

г) Система обеспечения инфраструктуры безопасности

22. Циклическая модель PDCA может быть применена к:

а) Все перечисленное

б) Системе обеспечение информационной безопасности

в) Система менеджмента информационной безопасности

г) Система менеджмента предприятия

д) Жизненному циклу продукта

23. Основными способами обработки рисков являются:

а) уменьшение рисков

б) передача рисков

в) избежание рисков

г) принятие рисков

д) ликвидация рисков

24. Не относится к политике ИБ утверждение:

а) Политика информационной безопасности должна быть краткой (лучшие практики указывают объем около 250 страниц)

б) Политика информационной безопасности должна быть реализуема (т.е. содержать только те положения, которые могут быть реализованы на практике), а ее реализация контролируема

в) Политика информационной безопасности должна устанавливать ответственность руководства и излагать подход организации к управлению ИБ

г) Пересмотренная политика информационной безопасности должна быть рассмотрена общем собрании коллектива

25. Не входит в жизненный цикл политики информационной безопасности этап:

а) разработка

б) внедрение

в) применение

г) аннулирование

д) обучение

е) анализ

Тест №2
Модуль 2. Государственная тайна

1. Закон, регулирующий отношения, возникающие в связи с отнесением сведений к государственной тайне, их засекречиванием или рассекречиванием и защитой в интересах обеспечения безопасности Российской Федерации называется:

а) Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне»;

б) Федеральный Закон РФ от 21.07.1993 N 5485-3 ФЗ «О государственной тайне»;

в) Закон РФ от 21.07.1993 N 5485-3 «О государственной тайне»;

г) Закон РФ от 21.07.1993 N 5485-1 «О государственной тайне и порядке засекречивания информации».

2. Государственная тайна это:

а) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности государства;

б) защищаемые государством сведения в области его военной, внешнеэкономической, разведывательно-диверсионной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности государства;

в) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной деятельности, распространение которых может нанести ущерб безопасности государства;

г) защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной деятельности, распространение которых может нанести ущерб безопасности государства.

3. Государственная тайна включает в себя:

а) тайну усыновления;

б) служебную тайну;

в) врачебную тайну;

г) все перечисленное.

4. Носители сведений, составляющих государственную тайну это:

а) материальные объекты, в которых сведения, составляющие государственную тайну, отображены в виде символов, образов, сигналов, технических решений и процессов;

б) материальные объекты и физические поля, в которых сведения, составляющие государственную тайну, отображены в виде символов, образов, сигналов, технических решений и процессов;

в) материальные объекты и физические поля, в которых сведения, составляющие государственную тайну, отображены в виде символов, образов, сигналов;

г) физические поля, в которых сведения, составляющие государственную тайну, отображены в виде символов, образов, сигналов, технических решений и процессов.

5. Совокупность органов защиты государственной тайны, используемых ими средств и методов защиты сведений, составляющих государственную тайну и их носителей, а также мероприятий, проводимых в этих цепях это:

а) средства защиты государственной тайны;

б) органы защиты государственной тайны;

в) методы защиты государственной тайны;

г) система защиты государственной тайны.

6. Санкционированное полномочным должностным лицом ознакомление конкретного лица со сведениями, составляющими государственную тайну:

а) допуск к государственной тайне;

б) разглашение государственной тайны;

в) доступ к сведениям, составляющим государственную тайну;

г) засекречивание сведений.

7. Категория, характеризующая важность информации, возможный ущерб вследствие ее разглашения, степень ограничения доступа к ней и уровень ее охраны государством называется:

а) степенью секретности

б) уровнем секретности

в) грифом секретности

г) допуском секретности

8. В Указе Президента РФ от 30.11.95 г. № 1203 утверждается:

а) перечень должностей, допущенных государственной тайне;

б) перечень сведений, отнесенных к государственной тайне;

в) перечень органов, допущенных к государственной тайне;

г) нет правильного ответа.

9. В Указе Президента РФ от 30.11.95 г. № 1203 не упоминается:

а) военная область;

б) область разведывательной, контрразведывательной, диверсионной и оперативно-розыскной деятельности;

в) область экономики, науки и техники;

г) область разведывательной, контрразведывательной и оперативно-розыскной деятельности.

10. Какая информация не может быть отнесена к государственной тайне:

а) о планах, организации, финансировании и материально- техническом обеспечении, средствах, формах, методах и, результатах разведывательной, контрразведывательной и оперативно-розыскной деятельности; о лицах, которые сотрудничают или ранее сотрудничали на конфиденциальной основе с органами, осуществляющими такую деятельность;

б) о директивах, планах, указаниях делегациям и должностным лицам по вопросам внешнеполитической и внешнеэкономической деятельности;

в) о содержании, объеме, финансировании и выполнении государственного оборонного заказа, а также о других особых мерах финансовой деятельности государства;

г) о неправомерных действиях государственных органов, органов местного и регионального самоуправления и должностных лиц.

11. Не включаются в перечень обязательных реквизитов, наносящихся на носители сведений, составляющих государственную тайну:

а) информация о степени секретности содержащихся в носителе сведений со ссылкой на соответствующий пункт действующего в данном органе государственной власти,

на данном предприятии или учреждении перечня сведений, подлежащих засекречиванию;

б) информация о органе государственной власти, о предприятии или учреждении, осуществивших засекречивание носителя;

в) регистрационный номер;

г) фамилия исполнителя, осуществившего засекречивание носителя.

12. Рассекречивание сведений, составляющих государственную тайну, осуществляется в случае:

а) приказа вышестоящего начальства;

б) изменения обстоятельств, вследствие которых дальнейшая защита сведений, составляющих государственную тайну, является нецелесообразной;

в) требования международной природоохранной организации;

г) личного желания исполнителя документа, содержащего сведения, составляющие государственную тайну.

13. Допуск должностных лиц и граждан к государственной тайне не предусматривает:

а) определение видов, объемов и порядка предоставления льгот, предусмотренных законом;

б) добровольный порядок оформления к допуску;

в) организационное обеспечение безопасности информации ограниченного доступа;

г) принудительный порядок оформления к допуску.

14. Наличие первая форма допуска к секретным сведениям дает право:

а) на ознакомление со сведениями особой важности, совершенно секретными и секретными;

б) на ознакомление только со сведениями особой важности;

в) на ознакомление со сведениями только совершенно секретными и секретными;

г) на ознакомление только с секретными сведениями.

15. Граждане, допущенные к государственной тайне, не могут быть ограничены в следующих правах:

а) права выезда за границу на срок, оговоренный в трудовом договоре (контракте) при оформлении допуска гражданина к государственной тайне;

б) права на изменения своего места проживания;

в) права на распространение сведений, составляющих государственную тайну, и на использование открытий и изобретений, содержащих такие сведения;

г) права на неприкосновенность частной жизни при проведении проверочных мероприятий в период оформления допуска к государственной тайне.

16. К секретным работам и документам допускаются лица:

а) имеющие психические заболевания;

б) нет правильного ответа;

в) понесшие уголовную ответственность;

г) имеющие постоянный контакт с родственниками за границей.

36. Режим секретности по содержанию не включает в себя порядок:

а) выполнения должностными лицами своих должностных обязанностей по сохранению государственных и служебных тайн, по соблюдению режима секретности;

б) обеспечения допуска к сведениям, относящимся к категории «для служебного доступа»;

в) установления степени секретности сведений, содержащихся в работах, документах и изделиях;

г) проведения служебных расследований по фактам разглашения секретных сведений.

17. Какое утверждение не относится к ПДТК:

а) занимается вопросами кадровой безопасности;

б) является консультативным органом при руководителе предприятия;

в) занимается вопросами режима секретности и противодействия иностранным техническим разведкам

г) является постоянно действующей технической комиссией

18. К принципам засекречивания информации не относится:

а) системность;

б) обоснованность;

в) законность;

г) своевременность.

19. К организационным и техническим методам и способам защиты государственной тайны относятся:

а) скрытие, ранжирование, дезинформация, дробление, учет, криптоанализ, шифрование;

б) скрытие, ранжирование, дезинформация, дробление, учет, кодирование, шифрование;

в) скрытие, ранжирование, дезинформация, диверсия, учет, кодирование, шифрование;

г) скрытие, ранжирование, дезинформация, синтез, учет, кодирование, шифрование.

20. К основным принципам учета засекреченной информации относится:

а) указание в учетах адреса, где был изготовлен носитель засекреченной информации;

б) групповая ответственность за сохранность каждого носителя защищаемой информации;

в) персональная материальная ответственность за утрату носителя защищаемой информации;

г) однократность регистрации конкретного носителя такой информации.

Тест № 3
Модуль 3. Нормативные правовые акты в области информационной безопасности

1. В состав процессов “PDCA” входят (по порядку):

а) План, Осуществление, Проверка, Действие

б) Планирование, Реализация, Выполнение, Контроль

в) План, Проверка, Контроль, Выпуск продукции

г) Проникновение, Реализация, Проверка, Действие

2. СОИБ означает:

а) Система обеспечения информационной безопасности

б) Собрание обозначений информационной безопасности

в) Создание объектов инфраструктуры безопасности

г) Система обеспечения инфраструктуры безопасности

3. Циклическая модель PDCA может быть применена к:

а) Все перечисленное

б) Системе обеспечение информационной безопасности

в) Система менеджмента информационной безопасности

г) Система менеджмента предприятия

Жизненному циклу продукта

4. Основными способами обработки рисков являются:

а) уменьшение рисков

б) **передача рисков**

в) **избежание рисков**

г) **принятие рисков**

д) ликвидация рисков

5. Не относится к политике ИБ утверждение:

а) Политика информационной безопасности должна быть краткой (лучшие практики указывают объем около 250 страниц)

б) Политика информационной безопасности должна быть реализуема (т.е. содержать только те положения, которые могут быть реализованы на практике), а ее реализация контролируема

в) Политика информационной безопасности должна устанавливать ответственность руководства и излагать подход организации к управлению ИБ

г) Пересмотренная политика информационной безопасности должна быть рассмотрена общем собрании коллектива

6. Не входит в жизненный цикл политики информационной безопасности этап:

а) разработка
б) внедрение
в) применение
г) аннулирование
д) обучение
е) анализ

7. Что является активом для организации в СМИБ?

а) Квалификация персонала
б) **Программное обеспечение**
в) **Имидж**
г) Коллективные мероприятия
д) Корпоративная политика

8. Управление информационной безопасностью организации включает в себя:

а) Осознание необходимости ИБ
б) **Оценку текущего состояния ИБ**
в) **Планирование мер по обработке рисков ИБ**
г) **Распределение ролей и ответственности в области ОИБ**
д) Обучение и мотивация сотрудников

9. В основные компоненты СУИБ входит:

а) Персонал
б) **Принципы управление ИБ**
в) **Ресурсы**
г) **Процессы и средства управления ИБ**
д) Инженерно–техническая защита ИС

10. В документацию СУИБ включают:

а) Рабочие инструкции
б) **Планы работ**
в) Статистику в области ИБ
г) **Документированные процедуры**

11. Количество этапов внедрения СУИБ, согласно ГОСТ Р ИСО/МЭК 27001 и немецкой методики IT-Grundschutz:

а) 9
б) 12
в) **14**
г) 10
д) 4
е) 11

12. Управление персоналом, физическая защита, поддержание работоспособности, реагирование на нарушения режима безопасности, планирование восстановительных работ, относятся к:

а) процедурному уровню
б) законодательному уровню
в) административному уровню
г) программно-техническому уровню

13. Политика ИБ предприятия относится к :

а) процедурному уровню
б) законодательному уровню
в) **административному уровню**
г) программно-техническому уровню.

14. Промежуток времени от момента, когда появляется возможность использовать слабое место, и до момента, когда пробел ликвидируется, называется:
а) форточкой безопасности
б) дверью угрозы
в) **окном опасности**
г) окном уязвимости

15. Попытка реализации действия, которое потенциально может привести к нарушению информационной безопасности, называется:
а) Угрозой
б) Уязвимостью
в) Источником угрозы
г) **Атакой**

16. Слабое место в информационной системе, которое может привести к нарушению безопасности путем реализации некоторой угрозы, называется:
а) Источником угрозы
б) Окном опасности
в) **Уязвимость**
г) Критичностью реализации угрозы.

17. Что не относится к этапам управления рисками:
а) инвентаризация анализируемых объектов
б) оценка рисков
в) **определение политики ИБ**
г) анализ угроз и их последствий

18. Для определения основных рисков необходимо следовать следующей цепочке:
а) источник угрозы > фактор (уязвимость) > угроза (действие) > последствия (атака)
б) источник угрозы > угроза (действие) > фактор (уязвимость) > последствия (атака)
в) источник угрозы > фактор (уязвимость) > последствия (атака) > угроза (действие)
г) угроза (действие) > фактор (уязвимость) > источник угрозы > последствия (атака)

19. Модель угроз это:
а) документ, определяющий перечень и характеристики основных (актуальных) угроз безопасности и уязвимостей при их обработке в ИС, которые должны учитываться в процессе организации защиты информации, проектирования и разработки систем защиты информации, проведения проверок (контроля) защищенности ИС
б) совокупность документированных руководящих принципов, правил, процедур и практических приёмов в области ИБ, которые регулируют управление, защиту и распределение ценной информации
в) комплекс политических, правовых, экономических, социально-культурных и организационных мероприятий государства, направленный на обеспечение конституционного права граждан на доступ к информации
г) Нет правильного ответа

20. Обеспечения ИБ предприятия включают в себя сочетание следующих уровней:
а) конфиденциальности, целостности и доступности информации
б) законодательного, научно-технического и физического
в) реализуемого, гибкого, гарантируемого и универсального
г) **законодательного, административного, процедурного и программно-технического**

21. ГОСТ Р ИСО/МЭК 27002-2012 это:

а) Международный стандарт качества

б) Российский стандарт качества

в) Международный стандарт – Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

г) Национальный стандарт РФ – Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

22. ISO/IEC 27002:2005 это:

а) Международный стандарт качества

б) Российский стандарт качества

в) Международный стандарт – Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

г) Национальный стандарт РФ – Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности

23. СТО ВР ИББС-1.0 относится к:

а) Международным стандартам

б) Национальным стандартам РФ

в) **Отраслевым стандартам РФ**

г) Ведомственным стандартам РФ

24. Категорирование активов компании заключается в:

а) оценки их критичности для обеспечения обороноспособности страны, так как бизнес-процессы вашей компания, не представляют ценности

б) оценки их стоимости в случае ликвидации предприятия

в) оценки их критичности, путем проведения референдума на предприятии

г) оценки их критичности для бизнес-процессов предприятия

25. Оценка критичности активов производится:

а) Только в условных денежных единицах

б) Только в долларах США

в) Только в рублях

г) **Как в денежных единицах, так и в уровнях**

Тест № 4
Модуль 4. Информационная безопасность в правоохранительных органах

1. Возможность за приемлемое время получить требуемую информационную услугу называется:

а) Конфиденциальность

б) Доступность

в) Целостность

г) Непрерывность

2. К аспектам информационной безопасности не относится:

а) Доступность

б) Целостность

в) Конфиденциальность

г) **Защищенность**

3. По каким критериям нельзя классифицировать угрозы:

а) по расположению источника угроз

б) по аспекту информационной безопасности, против которого угрозы направлены в

в) первую очередь

г) по способу предотвращения

в) по компонентам информационных систем, на которые угрозы нацелены

4. Главное достоинство парольной аутентификации – …

а) **простота**

б) надежность

в) секретность

г) запоминаемость

5. Сколько уровней включает в себя сетевая модель OSI?

а) 5

б) 7

в) 6

г) 8

6. Субъектами доступа могут являться:

а) процессы

б) пользователи

в) объекты доступа

г) ограждающие конструкции

7. На каком уровне сетевой модели OSI не работает межсетевой экран:

а) Физический

б) Сеансовый

в) Сетевой

г) Транспортный

8. Межсетевого экрана какого класса не существует:

а) экранирующий маршрутизатор

б) экранирующий коммутатор

в) экранирующий транспорт

г) экранирующий шлюз

9. Что из перечисленного не входит в состав программного комплекса антивирусной защиты:

а) Подсистема сканирования

б) Подсистема управления

в) Подсистема обнаружения вирусной активности

г) Подсистема устранения вирусной активности

10. На каком этапе заканчивается жизненный цикл автоматизированной системы?

а) Бета-тестирование системы

б) Внедрение финальной версии системы в эксплуатацию

в) Прекращение сопровождения и технической поддержки системы

г) Альфа-тестирование системы

11. Какие задачи выполняет теория защиты информации:

а) предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты

б) аккумулировать опыт предшествующего развития исследований, разработок и практического решения задач защиты информации

в) формировать научно обоснованные перспективные направления развития теории и практики защиты информации

г) выполняет все вышеперечисленные

12. Какой из протоколов не относится к протоколам защищенной передачи данных в сети Интернет:

а) SSL

б) SET

в) HTTP

г) IPSec

13. Какого метода разграничения доступа не существует:

а) разграничение доступа по спискам

б) разграничение доступа по уровням секретности и категориям

в) локальное разграничение доступа

г) парольное разграничение доступа

14. К основным функциям подсистемы защиты операционной системы относятся:

а) идентификация, аутентификация, авторизация, управление политикой безопасности и разграничение доступа

б) криптографические функции

в) сетевые функции

г) все вышеперечисленные

15. Риск – это…

а) вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки

б) фактическая оценка величины ущерба, который понес владелец информационного ресурса в результате успешно проведенной атаки

в) действие, которое направлено на нарушение конфиденциальности, целостности и/или доступности информации, а также на нелегальное использование других ресурсов сети

г) реализованная угроза

16. Основные угрозы доступности информации:

а) непреднамеренные ошибки пользователей

б) злонамеренное изменение данных

в) хакерская атака

г) отказ программного и аппаратного обеспечения

д) разрушение или повреждение помещений

е) перехват данных

17. Информационная безопасность автоматизированной системы – это состояние автоматизированной системы, при котором она, …

а) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой — ее наличие и функционирование не создает информационных угроз для элементов самой системы и внешней среды

б) с одной стороны, способна противостоять воздействию внешних и внутренних информационных угроз, а с другой – затраты на её функционирование ниже, чем предполагаемый ущерб от утечки защищаемой информации

в) способна противостоять только информационным угрозам, как внешним так и внутренним

г) способна противостоять только внешним информационным угрозам.

18. Под угрозой удаленного администрирования в компьютерной сети понимается угроза …

а) несанкционированного управления удаленным компьютером

б) внедрения агрессивного программного кода в рамках активных объектов Web-в) страниц

г) перехвата или подмены данных на путях транспортировки

д) вмешательства в личную жизнь

е) поставки неприемлемого содержания

19. Сервисы безопасности включают в себя:

а) идентификация и аутентификация

б) шифрование

в) инверсия паролей

г) контроль целостности

д) регулирование конфликтов

е) экранирование

ж) обеспечение безопасного восстановления

з) кэширование записей

20. Методы повышения достоверности входных данных

а) Замена процесса ввода значения процессом выбора значения из предлагаемого множества

б) Отказ от использования данных

в) Проведение комплекса регламентных работ

г) Использование вместо ввода значения его считывание с машиночитаемого носителя

д) Введение избыточности в документ первоисточник

е) Многократный ввод данных и сличение введенных значений

21. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ):

а) МЭ были разработаны для активной или пассивной защиты, а СОВ – для активного или пассивного обнаружения

б) МЭ были разработаны для активного или пассивного обнаружения, а СОВ – для активной или пассивной защиты

в) МЭ работают только на сетевом уровне, а СОВ – еще и на физическом

22. В соответствии с нормами российского законодательства защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

а) обеспечение защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также от иных неправомерных действий в отношении такой информации

б) реализацию права на доступ к информации»

в) соблюдение норм международного права в сфере информационной безопасности

г) выявление нарушителей и привлечение их к ответственности

д) соблюдение конфиденциальности информации ограниченного доступа

е) разработку методов и усовершенствование средств информационной безопасности

23. Причины возникновения ошибки в данных

а) Погрешность измерений

б) Ошибка при записи результатов измерений в промежуточный документ

в) Неверная интерпретация данных

г) Ошибки при переносе данных с промежуточного документа в компьютер

д) Использование недопустимых методов анализа данных

е) Неустранимые причины природного характера

ж) Преднамеренное искажение данных

з) Ошибки при идентификации объекта или субъекта хозяйственной деятельности

24. Средства защиты объектов файловой системы основаны на

а) определении прав пользователя на операции с файлами и каталогами

б) задании атрибутов файлов и каталогов, независящих от прав пользователей

в) установки шлагбаумов на входе в контролируемую зону объекта информатизации

г) нет правильного ответа

25. Суть компрометации информации:

а) внесение изменений в базу данных, в результате чего пользователь лишается доступа к информации

б) несанкционированный доступ к передаваемой информации по каналам связи и уничтожения содержания передаваемых сообщений

в) внесение несанкционированных изменений в базу данных, в результате чего потребитель вынужден либо отказаться от неё, либо предпринимать дополнительные усилия для выявления изменений и восстановления истинных сведений

Критерии оценки тестовых заданий

Структура работы	Критерии оценки	Распределение баллов
Один вопрос теста (25 вопросов в варианте)	Неправильный ответ / Правильный ответ	
Модуль 1		0,8
Модуль 2		0,88
Модуль 3		0,32
Модуль 4		0,24

Практические работы

Цель проведения практической работы – оценка уровня владения базовой профессиональной терминологией в сфере государственного и муниципального управления. Практическая работа проводится в письменной форме.

Темы практических работ

Модуль 1. Представление информации.

1. Информация и данные. Адекватность информации.
2. Кодирование при передаче и хранении информации.
3. Роль средств массовой информации.
4. Информационные ресурсы.
5. Методы классификации.

Модуль 2. Прикладное программное обеспечение

6. Принципы работы в текстовом процессоре Microsoft Word 2010.
7. Принципы работы в табличном процессоре Microsoft Excel 2010.
8. Органайзер. Характеристика органайзера Microsoft Outlook.
9. Работа с программой мультимедиа-презентаций Microsoft PowerPoint 2010.

Модуль 3. Знания и информационные системы

10. Этапы развития информационных систем.
11. Инструментарий информационной технологии.
12. Элементы информационных систем.
13. Жизненный цикл информации в информационных системах.

Модуль 4. Информационные системы в обеспечении правоохранительной деятельности

14. История криминалистических учетов.
15. Оперативно–розыскные мероприятия, проводимые по санкции суда.
16. Оперативно–розыскные мероприятия, проводимые по ведомственным санкциям.
17. Обеспечение информационных систем, используемых в правоохранительной деятельности.

Практическая работа №1

Модуль 1. Защита государственной и коммерческой тайны в системе защиты информации

1. Прочитайте и проанализируйте Доктрину ИБ РФ.
2. Постройте схему органов государственной власти и самоуправления, отвечающих за информационную безопасность.
3. Определите функциональные обязанности органов государственной власти и самоуправления, отвечающих за информационную безопасность.
4. Определите положения государственной политики в области обеспечения ИБ.
5. Выделите первоочередные мероприятия по обеспечению ИБ, дайте им оценку.

Практическая работа №10

Модуль 3. Нормативные правовые акты в области информационной безопасности

1. Самостоятельно изучите ГОСТ Р ИСО/МЭК 27000-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология» и ГОСТ Р 58545-2019 «Менеджмент знаний. Руководящие указания по сбору, классификации, маркировке и обработке информации».
2. Назовите область применения ГОСТ Р ИСО/МЭК 27000-2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Системы менеджмента информационной безопасности. Общий обзор и терминология».
3. Назовите определение термина «актив».
4. Что такое контроль доступа с точки зрения ГОСТ Р ИСО/МЭК 27000-2012?
5. Что такое событие с точки зрения ГОСТ Р ИСО/МЭК 27000-2012?
6. Назовите определение термина «система менеджмента информационной безопасности».

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	 0/3/ 6 0/3/7 0/4/8 0/3/6

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. Ковалев, Д.В. Информационная безопасность : учебное пособие / Д.В. Ковалев, Е.А. Богданова ; Министерство образования и науки РФ, Южный федеральный университет. - Ростов-на-Дону : Издательство Южного федерального университета, 2016. - 74 с. : схем., табл., ил. - Библиогр. в кн. - ISBN 978-5-9275-2364-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=493175.

2. Малюк, А.А. Защита информации в информационном обществе : учебное пособие / А.А. Малюк. - Москва : Горячая линия-Телеком, 2015. - 229 с. : ил., схем., табл. - Библиогр. в кн. - ISBN 978-5-9912-0481-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=457170

Дополнительная литература

3. Милославская, Н.Г. Управление инцидентами информационной безопасности и непрерывностью бизнеса : учебное пособие для вузов / Н.Г. Милославская, М.Ю. Сенаторов, А.И. Толстой. - Москва : Горячая линия - Телеком, 2013. - 170 с. : ил. - (Вопросы управления информационной безопасностью. Вып. 3). - Библиогр. в кн. - ISBN 978-5-9912-0273-2 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=253577

4. Шилов, А.К. Управление информационной безопасностью : учебное пособие / А.К. Шилов ; Министерство науки и высшего образования РФ, Федеральное государственное автономное образовательное учреждение высшего образования «Южный федеральный

университет», Институт компьютерных технологий и информационной безопасности. - Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2018. - 121 с. : ил. - Библиогр.: с. 81 - 82 - ISBN 978-5-9275-2742-7 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=500065.

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 курсового проектирования (выполнения курсовых работ):*** аудитория № 613 (гуманитарный корпус). **4.** ***учебная аудитория для проведения групповых и индивидуальных консультаций:***	Лекции, практические занятия, текущий контроль, промежуточная аттестация, экзамен	**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 AKG WMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром Promethean ActivBoard 387 RPO MOUNT EST -1 шт., Ком-ер встраиваемый в кафедру INTEL Core i3-4150/DDr3 4 Gb/HDD, Экран настенный Draper Luma AV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H – 1 шт. , Мультимедиа-проектор Panasonic PT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKG WMS45 – 1 шт. , Терминал видео конференц-связи LifeSize Icon 600 Camera 10x Phone 2nd Generation – 1 шт., Экран настенный Draper Luma AV(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** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование:

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.** ***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). **6.** ***помещения для самостоятельной работы:*** аудитория № 613 (гуманитарный корпус), читальный зал библиотеки аудитория 402 (гуманитарный корпус).		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.
Наименование специализированных аудиторий, кабинетов,	Вид занятий	Наименование оборудования, программного обеспечения

лабораторий		
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), компьютерный класс аудитория № 420 (гуманитарный корпус). **4. *учебная аудитория для текущего контроля***	Лекции, практические занятия, текущий контроль, промежуточная аттестация	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **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 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.

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).		**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 **Информационная безопасность в правоохранительной сфере** на 7 семестр
___очная_ф/о___

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	56,2
лекций	18
практических/ семинарских	18
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)	108
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на подготовку к зачету (Контроль)	–

Форма контроля
Зачет 7 семестр

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Информационная безопасность в правоохранительной сфере** на 8 семестр
очная ф/о

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	33,2
лекций	16
практических/ семинарских	16
лабораторных	–
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на самостоятельную работу обучающихся (СР)	38,8
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на подготовку к экзамену (Контроль)	36

Форма контроля
Экзамен 8 семестр

Семестр 7

№	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. Защита государственной и коммерческой тайны в системе защиты информации Тема: Понятие и защита государственной и коммерческой тайны в системе защиты информации. Принципы защиты защита государственной и коммерческой тайны. Отнесение сведений к коммерческой, служебной и профессиональной тайнам. Правовой режим информационных ресурсов. Признаки охраноспособности информации. Цели защиты информации. Режим защиты информации. Тема: Виды защищаемой информации. Федеральный закон от 27.07.2006 N 149-ФЗ «Об информации, информационных технологиях и о защите информации». Общедоступная информация. Ограничение доступа к информации. Конфиденциальная информация. Тема: Виды тайн в российском законодательстве. Персональные данные. Федеральный закон от 27.07.2006 N 152-ФЗ «О персональных данных». Защита коммерческой тайны. Федеральный закон от 29.07.2004 N 98-ФЗ «О коммерческой тайне». Юридические меры защиты коммерческой тайны. Административно-организационные меры защиты коммерческой тайны. Социально-психологические меры защиты коммерческой тайны. Технические средства защиты коммерческой тайны. Тема: Служебная тайна. Признаки профессиональной тайны. Тайна в юридической практике. Тайна в сфере экономической деятельности. Тайна, связанная с этическими соображениями.	2 2 2 2	2 2 4		13 13 13 13	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, лабораторная работа
2	Модуль 2. Государственная тайна Тема: Государственная тайна и порядок отнесения к ней информации. Закон РФ от 21.7.93 г. № 5485-1 «О государственной	2	2		14	Самостоятельное изучение	Тест, лабораторная работа

	тайне» Засекречивание сведений, составляющих государственную тайну. Рассекречивание сведений, составляющих государственную тайну. Допуск к государственной тайне. Защита государственной тайны. Организация режима секретности, его особенности и содержание. Организационные и технические способы защиты государственной тайны.	2 2 2	 2 4		14 14 14	рекомендуемой основной и дополнительной литературы	
	Всего часов	16	16	–	108		

Семестр 8

№	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. Нормативные правовые акты в области информационной безопасности					Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа
	Основные нормативные правовые акты в области информационной безопасности и защиты информации. Отечественные и зарубежные стандарты в области информационной безопасности. ГОСТ Р 50922-2006 — Защита информации. Основные термины и определения.	2	2		5		
	ГОСТ Р 50.1.053-2005 — Информационные технологии. Основные термины и определения в области технической защиты информации. ГОСТ Р 51188—98 — Защита информации. Испытание программных средств на наличие компьютерных вирусов. Типовое руководство. ГОСТ Р 51275-2006 — Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. ГОСТ Р ИСО/МЭК 15408-1-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель. ГОСТ Р ИСО/МЭК 15408-2-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 2. Функциональные требования безопасности	2	2		5		

	ГОСТ Р ИСО/МЭК 15408-3-2008 — Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 3. Требования доверия к безопасности. ГОСТ Р ИСО/МЭК 15408 — «Общие критерии оценки безопасности информационных технологий» — стандарт, определяющий инструменты и методику оценки безопасности информационных продуктов и систем; он содержит перечень требований, по которым можно сравнивать результаты независимых оценок безопасности — благодаря чему потребитель принимает решение о безопасности продуктов. Сфера приложения «Общих критериев» — защита информации от несанкционированного доступа, модификации или утечки, и другие способы защиты, реализуемые аппаратными и программными средствами.	2	2		5		
	ГОСТ Р ИСО/МЭК 17799 — «Информационные технологии. Практические правила управления информационной безопасностью». ISO/IEC 17799:2005. ГОСТ Р ИСО/МЭК 27001 — «Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования».Прямое применение международного стандарта с дополнением —Прямое применение международного стандарта — ISO/IEC 27001:2005. ГОСТ Р 51898-2002 — Аспекты безопасности. Правила включения в стандарты. РД СВТ. Защита от НСД. Показатели защищенности от НСД к информации — содержит описание показателей защищенности информационных систем и требования к классам защищенности.	2	2		5		
2	Модуль 4. Информационная безопасность в правоохранительных органах. Доктрина информационной безопасности Российской Федерации. Единая система информационно-аналитического обеспечения деятельности МВД России. Основные задачи обеспечения информационной безопасности в правоохранительных органах. Угрозы по добыванию, обработке и использованию оперативно-розыскной информации. Виды категорируемых объектов информации в правоохранительных органах. Специальная проверка. Специальное исследование объекта защиты информации. Специальное обследование. Вопросы безопасности, связанные с персоналом. Соглашения о конфиденциальности. Особенности работы с персоналом, владеющим конфиденциальной информацией. Подбор и подготовка кадров. Проверка персонала на благонадежность. Принципы построения разрешительной системы доступа. Доступ к отчуждаемым носителям конфиденциальной информации. Доступ к средствам вычислительной техники, обрабатывающей конфиденциальную информацию. Текущая работа с персоналом, владеющим конфиденциальной информацией. Служебное расследование. Особенности увольнения	2	2		5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	Тест, практическая работа

	сотрудников, владеющих конфиденциальной информацией. Одностороннее соглашение о неразглашении. Взаимное соглашение о неразглашении. Распространенные недостатки соглашений о неразглашении.						
	Виды компьютерной преступности в сфере вычислительных сетей. Способы совершения компьютерных преступлений. Ответственность за компьютерные преступления. Методика раскрытия и расследования компьютерных преступлений. Типичные следственные ситуации первоначального этапа и следственные действия в расследовании компьютерных преступлений. Поиск и изъятие информации и следов воздействия на нее в ЭВМ и ее устройствах. Использование специальных познаний и назначение экспертиз. Организация противодействия компьютерной преступности.	2	2		5		
	Понятие информационной безопасности. Термины и определения. Система информационной безопасности. Проверка безопасности информационных систем. Аудит систем. Общие сведения об информационной безопасности. Проверка безопасности информационных систем. Мониторинг систем. Основные составляющие информационной безопасности. Внешний аудит. Обоснование необходимости рассмотрения вопросов информационной безопасности. Внутренний аудит. Процессный подход в рамках управления ИБ. Проблемы построения современных систем безопасности. Слежение за доступом к системам и их использованием. Оценка рисков нарушения безопасности. Средства управления информационной безопасностью. Защита от вредоносного программного обеспечения. Ключевые средства контроля информационной безопасности. Ответственность за информационные ресурсы. Требование бизнеса по обеспечению контроля доступа. Факторы, необходимые для успешной реализации системы информационной безопасности в организации. Управление доступом пользователей. Обязанности пользователей. Группы требований к информационной безопасности организации. Система планирования бесперебойной работы организации. Политика информационной безопасности.	2	2		5		
	Классификация информации. Инфраструктура информационной безопасности. Безопасность информации в должностных инструкциях. Обучение пользователей правилам информационной безопасности. Реагирование на события, таящие угрозу безопасности. Оперирование с носителями информации и их защита. Термины и определения управления информационной безопасностью. Понятие управления информационной безопасностью Циклическая модель улучшения процессов.	2	2		3,8		
	Всего часов за семестр	16	16	0	36		
	Всего часов	34	34	0	147		