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
Безопасность критической информационной инфраструктуры

Часть, формируемая участниками образовательных отношений (Б1.В.06)

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 4
2. Цель и место дисциплины в структуре образовательной программы 5
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся) 5
4. Фонд оценочных средств по дисциплине 5

   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. 5

   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. 8
5. Учебно-методическое и информационное обеспечение дисциплины 17

   5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины 17

   5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы 18
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине 20

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**
Организационно-управленческая	ПК-1. Способен формировать требования по защите информации и политики безопасности компьютерных систем и сетей.	ПК-1.1 Знает основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Знать основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.
		ПК-1.2 Умеет применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Уметь применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.
		ПК-1.3 Владеет методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Владеть методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.
Эксплуатационная	ПК-2. Способен проводить мероприятия по оценке защищенности компьютерных систем и сетей.	ПК-2.1 Знает основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.	Знать основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.
		ПК-2.2 Умеет проводить мероприятия по оценке защищенности компьютерных систем и сетей.	Уметь проводить мероприятия по оценке защищенности компьютерных систем и сетей.

		ПК-2.3 Владеет методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.	Владеть Владеет методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Безопасность критической информационной инфраструктуры» относится к части, формируемой участниками образовательных отношений.

Дисциплина изучается на 5 курсе в 9 семестре.

Целью учебной дисциплины «Безопасность критической информационной инфраструктуры», является формирование навыков определения основных угрозы безопасности информации, проведения мероприятий по оценке защищенности и формировать требования по защите информации и политики безопасности на объектах критической информационной инфраструктуры.

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

Содержание рабочей программы представлено в Приложении № 1.

4. Фонд оценочных средств по дисциплине

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

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

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ПК-1.1 Знает основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Знать основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Не знает или показывает очень слабые знания.	Знает некоторые основные принципы, методы и этапы формирования требования по защите	Знает некоторые основные принципы, методы и этапы формирования требования по защите	Знает основные принципы, методы и этапы формирования требования по защите информации и

			информации и политики безопасности компьютерных систем и сетей, но допускает ошибки при их применении.	информации и политики безопасности компьютерных систем и сетей.	политики безопасности компьютерных систем и сетей.
ПК-1.2 Умеет применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Уметь применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Не умеет.	Умеет применять некоторые основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей., но допускает ошибки при их применении.	Умеет применять некоторые основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Умеет применять основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.
ПК-1.3 Владеет методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Владеть методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Не владеет.	Владеет основными элементами методики формирования требований по защите информации и	Владеет основными элементами методики формирования требований по защите информации и	Владеет методикой формирования требований по защите информации и политики безопасности

			политики безопасности компьютерных систем и сетей, но допускает ошибки при их использовании.	политики безопасности компьютерных систем и сетей.	компьютерных систем и сетей.

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

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ПК-2.1 Знает основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.	Знать основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.	Не знает или показывает очень слабые знания.	Знает некоторые основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения, но делает ошибки при их выборе.	Знает некоторые основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.	Знает основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.
ПК-2.2 Умеет проводить мероприятия по оценке защищенности компьютерных систем и сетей.	Уметь проводить мероприятия по оценке защищенности компьютерных систем и сетей.	Не умеет.	Умеет проводить основные мероприятия по оценке защищенности компьютерных систем и сетей, но	Умеет проводить основные мероприятия по оценке защищенности компьютерных систем и сетей.	Умеет проводить мероприятия по оценке защищенности компьютерных систем и сетей.

			делает ошибки при их использовании.		
ПК-2.3 Владеет методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.	Владеть методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.	Не владеет.	Владеет основными методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей, но делает ошибки при их использовании.	Владеет основными методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.	Владеет методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.

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

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

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ПК-1.1 Знает основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	Знать основные принципы, методы и этапы формирования требования по защите информации и политики безопасности компьютерных систем и сетей.	тестирование, практическое задание; лабораторная работа
ПК-1.2 Умеет применять основные принципы, методы и этапы формирования требования по защите информации и	Уметь применять основные принципы, методы и этапы формирования требования по защите информации и политики	тестирование, практическое задание; лабораторная работа

политики безопасности компьютерных систем и сетей.	безопасности компьютерных систем и сетей.	
ПК-1.3 Владеет методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	Владеть методикой формирования требований по защите информации и политики безопасности компьютерных систем и сетей.	тестирование, практическое задание; лабораторная работа

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

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
ПК-2.1 Знает основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.	Знать основные мероприятия по оценке защищенности компьютерных систем и сетей, методы и принципы их проведения.	тестирование, практическое задание; лабораторная работа
ПК-2.2 Умеет проводить мероприятия по оценке защищенности компьютерных систем и сетей.	Уметь проводить мероприятия по оценке защищенности компьютерных систем и сетей.	тестирование, практическое задание; лабораторная работа
ПК-2.3 Владеет методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.	Владеть методами и принципами проведения мероприятия по оценке защищенности компьютерных систем и сетей.	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
«Безопасность критической информационной инфраструктуры»

Специальность: 10.05.05 Безопасность информационных технологий в правоохранительной сфере

курс 5, семестр 9

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1. Основная проблематика безопасности критической информационной инфраструктуры.				
Текущий контроль				
Лабораторная работа	5	1	0	5
Практическая работа	5	5	0	25
Рубежный контроль				
Тест	10	1	0	10
Всего			0	40
Модуль 2. Создание системы защиты информации в критической информационной инфраструктуре.				
Текущий контроль				
Лабораторная работа	4	3	0	12
Практическая работа	3	4	0	12
Рубежный контроль				
Тест	6	1	0	6
Всего			0	30
Поощрительные баллы				
1. Участие в студенческой олимпиаде по дисциплине	3	1	0	3
2.Публикация научной статьи	4	1	0	4
3.Участие в научно-практической конференции по профилю	3	1	0	3
Всего		3	0	10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий			0	-6
2. Посещение практических (семинарских, лабораторных занятий)			0	-10
Итоговый контроль				
1.Экзамен	30	1	0	30

Экзамен

Структура экзаменационного билета

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

Экзаменационные материалы

1. Основные понятия, определения и термины ИБ КИИ.
2. Сфера действия Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.
3. Правовое регулирование ИБ КИИ.
4. Принципы обеспечения безопасности КИИ.
5. Состав сил и средств, предназначенных для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.
6. Национальный координационный центр по компьютерным инцидентам.
7. Реестр значимых объектов КИИ.
8. Полномочия Президента Российской Федерации и органов государственной власти Российской Федерации в области ОБ КИИ (Правительство РФ, ФСБ России, ФСТЭК России и Министерства связи и массовых коммуникаций).
9. Перечень информации, представляемой в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.
10. Порядок представления информации в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.
11. Порядок обмена информацией о компьютерных инцидентах на объектах КИИ.
12. Права и обязанности субъектов критической информационной инфраструктуры.
13. Оценка безопасности критической информационной инфраструктуры.
14. Государственный контроль в области обеспечения безопасности значимых объектов критической информационной инфраструктуры.
15. Ответственность за нарушение требований Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 № 187-ФЗ.
16. Категории значимости объектов КИИ.
17. Виды критериев и порядок отнесения объектов КИИ к категориям значимости.
18. Представление информации в реестр и ведение реестра значимых объектов КИИ.
19. Формы направления сведений о результатах категорирования объектов КИИ.
20. Порядок и основания изменения категорий значимости объектов КИИ.
21. Основные задачи системы безопасности (предотвращение неправомерного доступа, а также иных неправомерных действий в отношении такой информации; недопущение воздействия на технические средства обработки информации; восстановление функционирования значимого объекта; непрерывное взаимодействие с государственной системой).
22. Угрозы безопасности КИИ.
23. Требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования.
24. Требования к силам обеспечения безопасности значимых объектов критической информационной инфраструктуры.
25. Требования к программным и программно-аппаратным средствам, применяемым для обеспечения безопасности значимых объектов критической информационной инфраструктуры.
26. Угрозы безопасности КИИ.
27. Требования к организационно-распорядительным документам по безопасности значимых объектов.
28. Требования к функционированию системы безопасности в части организации работ по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

29. Требования к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов.
30. Установление требований к обеспечению безопасности значимого объекта.
31. Разработка организационных и технических мер по обеспечению безопасности значимого объекта.
32. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие.
33. Обеспечение безопасности значимого объекта в ходе его эксплуатации.
34. Обеспечение безопасности значимого объекта при выводе его из эксплуатации.
35. Требования к организационным и техническим мерам, принимаемым для обеспечения безопасности значимых объектов.
36. Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости.
37. Назначение (цели создания) ГосСОПКА.
38. Принципы создания и функционирования ГосСОПКА.
39. Территориальная структура ГосСОПКА.
40. Основные задачи центров ГосСОПКА.
41. Виды обеспечения функционирования ГосСОПКА.
42. Положение о НКЦКИ.
43. Перечень и порядок представления информации в ГосСОПКА.
44. Сроки предоставления информации.
45. Порядок обмена информацией о компьютерных инцидентах.
46. Центры ГосСОПКА.
47. Создание центра ГосСОПКА.
48. Классификация центров ГосСОПКА.
49. Функции ГосСОПКА
50. Организация взаимодействия сегмента ГосСОПКА с НКЦКИ ГосСОПКА.
51. Способы взаимодействия сегмента ГосСОПКА с НКЦКИ ГосСОПКА.
52. Порядок предоставления сведений в НКЦКИ ГосСОПКАК.
53. Перечень передаваемой информации о компьютерных атаках.
54. Перечень предоставляемой информации о защищенности информационных ресурсов.
55. Перечень предоставляемой информации о защищенности информационных ресурсов, доступных из сети Интернет.
56. Создание своего центра ГосСОПКА
57. Инфраструктура для подключения к ГосСОПКА
58. Реализация общей концепции ИБ организации. Выстраивание процессов обеспечения информационной безопасности организации КИИ.
59. Определение вида и типа программных, программно–аппаратных средств защиты информации, обеспечивающих реализацию технических мер по защите значимого объекта КИИ.
60. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие.

Пример экзаменационного билета:

Форма 1.4.-33

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

Специальность 10.05.05 Безопасность информационных технологий в правоохранительной сфере

Дисциплина Безопасность критической информационной инфраструктуры

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

1.Правовое регулирование ИБ КИИ.

2. Внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввод его в действие.

Зав. Кафедрой УИБ А.С. Исмагилова

Критерии оценивания результатов экзамена для ОФО:

Критерии оценки (в баллах):

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

- 17-24 баллов выставляется студенту, если студент раскрыл в основном теоретические вопросы, однако допущены неточности в определении основных понятий. При ответе на дополнительные вопросы допущены небольшие неточности.

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

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

Устанавливается следующая градация перевода оценки из многобалльной в четырехбалльную:

Экзамены:

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

Примерная тематика курсовых проектов (работ)

Курсовое проектирование не предусмотрено

Тестовые задания

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

Модуль 1. Основная проблематика безопасности критических информационной инфраструктуры.Полномочия ФСТЭК в отношении безопасности КИИ

а) Утверждение формы направления сведений о результатах категоризации объектов КИИ
б) Установление требований по обеспечению безопасности значимых объектов КИИ и к созданию систем безопасности таких объектов
в) Внесение предложений о совершенствовании нормативно-правового регулирования
г) Правовое регулирование деятельности Национального координационного центра по компьютерным инцидентам и координация действий субъектов КИИ

1. Полномочия ФСБ в отношении безопасности КИИ
а) Утверждение формы направления сведений о результатах категоризации объектов КИИ
б) Установление требований по обеспечению безопасности значимых объектов КИИ и к созданию систем безопасности таких объектов
в) Внесение предложений о совершенствовании нормативно-правового регулирования
г) Правовое регулирование деятельности Национального координационного центра по компьютерным инцидентам и координация действий субъектов КИИ

Модуль 2. Создание системы защиты информации в критической информационной инфраструктуре.

1. Обязанности субъектов КИИ в отношении ФЗ
№ 187 а) Провести категорирование объектов
КИИ
б) Обеспечить интеграцию в ГосСОПКА
в) Обеспечить безопасности объектов КИИ посредством внедрения организационных и технических мер
г) Внести предложения о совершенствовании нормативно-правового регулирования

2. К организационным методам обеспечения информационной безопасности критической информационной инфраструктуры относятся:
а) Организация внутри объектового и пропускного режима и
охраны б) Комплексное планирование мероприятий по защите
информации в) Лицензионные соглашения и контракты
г) Меры ответственности за нарушение правил защиты

Критерии оценки тестовых заданий

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

Лабораторные работы

Цель проведения лабораторных работы – практическое освоение материала дисциплины.

Темы лабораторных работ

Модуль 1. Основная проблематика безопасности критическойх информационной инфраструктуры.

1) Правовые основы понятия критической информационной инфраструктуры.

Модуль 2. Создание системы защиты информации в критической информационной инфраструктуре

2) Модель угроз объектов критической информационной инфраструктуры.

3) Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры.

4) Формирование технического проекта. Разработка эксплуатационной документации.

Лабораторная работа №6

Модуль 1. Представление информации

Тема: Правовые основы понятия критической информационной инфраструктуры.

Цель: Изучить основные нормативно–правовые акты, регламентирующие требования к информационной безопасности КИИ.

Задание: Изучить постановления Правительства РФ от 08.02.2018 года № 127 «Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений».

Критерии оценки лабораторной работы

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

Практические работы

Цель проведения практических работ – практическое освоение материала дисциплины.

Темы практических работ

Модуль 1. Основная проблематика безопасности критической информационной инфраструктуры.

1.Правовые основы понятия критической информационной инфраструктуры.

2. Методы обеспечения информационной безопасности критической информационной инфраструктуры.

3. Принципы обеспечения комплексной безопасности критической информационной инфраструктуры.

4. Уязвимости и угрозы безопасности организации.

Модуль 2. Создание системы защиты информации в критической информационной инфраструктуре.

5. Выявление критических процессов и определение объектов критической информационной инфраструктуры организации.
6. Модель актуальных угроз безопасности объектов критической инфраструктуры организации.
7. Категорирование объектов критической информационной инфраструктуры организации.
8. Комплекс мер и методов обеспечения информационной безопасности.
9. Нейтрализация актуальных угроз.

Практическая работа № 1

Модуль 1. Представление информации

Тема: Правовые основы понятия критической информационной инфраструктуры.

Цель: Изучить основные нормативно–правовые акты, регламентирующие требования к информационной безопасности КИИ.

Задание: Изучить Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

Порядок выполнения:

1. Изучить Федеральный закон от 26 июля 2017 г. N 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
2. Ответить на контрольные вопросы:

a) Назовите принципы обеспечения безопасности критической информационной инфраструктуры.
b) Что относится к силам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.
c) Что относится к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты.
d) Какие действия осуществляются в государственной системе обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации.
e) Исходя из чего проводится категорирование объектов критической информационной инфраструктуры.
f) В какой срок и кем проводится проверка соблюдения порядка осуществления категорирования и правильность присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо неприсвоения ему ни одной из таких категорий.
g) Какие сведения вносятся в Реестр значимых объектов критической информационной инфраструктуры.
h) Перечислите права субъектов критической информационной инфраструктуры.
i) Перечислите обязанности субъектов критической информационной инфраструктуры.
j) Перечислите основные задачи системы безопасности значимого объекта критической информационной инфраструктуры.
k) Что предусматривают требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры, устанавливаемые федеральным органом исполнительной власти, уполномоченным в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.
l) Что анализируется при осуществлении оценки безопасности критической информационной инфраструктуры.

Критерии оценки практической работы

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

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература

1. О безопасности критической информационной инфраструктуры Российской Федерации: Федеральный закон (от 26.07.2017 № 187-ФЗ) [Электронный ресурс] : сайт Президента Российской Федерации: http://www.kremlin.ru/acts/bank/42489
2. Об информации, информационных технологиях и о защите информации: Федеральный Закон (от 27 июля 2006 г. № 149-ФЗ) [Электронный ресурс]: справочная правовая система: http://www.consultant.ru/document/cons_doc_LAW_61798/
3. Об утверждении порядка ведения реестра значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК России (от 06.12.2017 № 227) [Электронный ресурс] : сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/normotvorcheskaya/akty/53- prikazy/1587-prikaz-fstek-rossii-ot-6-dekabrya-2017-g-n-227
4. Об утверждении Правил категорирования объектов критической информационной инфраструктуры Российской Федерации, а также перечня показателей критериев значимости объектов критической информационной инфраструктуры Российской Федерации и их значений: Постановление Правительства РФ (от 8 февраля 2018 г. № 127) [Электронный ресурс] : информационно-правовой портал: http://www.garant.ru/products/ipo/prime/doc/71776120/
5. Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Постановление Правительства Российской Федерации (от 17.02.2018 г. № 162) [Электронный ресурс], информационно-правовой портал: http://www.garant.ru/products/ipo/prime/doc/71783452/
6. Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования: Приказ ФСТЭК (от 21.12.2017 №235) [Электронный ресурс] : сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/index?id=1606:prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235
7. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК (от 25.12.2017 № 239) [Электронный ресурс] : сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239
8. Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов

критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК России (от 11.12.2017 № 229) [Электронный ресурс]: сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1475-prikaz-fstek-rossii-ot-11-

9. Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий: Приказ ФСТЭК России (от 22.12.2017 № 236) [Электронный ресурс] : сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/index?id=1607:prikaz-fstek-rossii-ot-22-dekabrya-2017-g-n-236

10. О персональных данных: Федеральный Закон (от 27 июля 2006 г. №152-ФЗ) [Электронный ресурс] : справочная правовая система: http://www.consultant.ru/document/Cons_doc_LAW_61801/

Дополнительная литература

11. Кудрявцев А.М. Киберустойчивость информационно-телекоммуникационной сети / М.А. Коцыняк, И.А. Кулешов, А.М. Кудрявцев, О.С. Лаутаи. – СПб.: Бостон-спектр, 2015. – 150 с.

12. Чукарин А.В. Бизнес-процессы и информационные технологии в управлении современной инфокоммуникационной компанией / А.В. Чукарин. – М.: Альпина Паблишер. – 2016. - 512 с.

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

1. Электронная библиотечная система «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. ***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), Лаборатория систем и сетей передачи данных, сетей и систем передачи информации,	Лекции, практические занятия, лабораторные занятия, курсовое проектирование (выполнение курсовых работ), групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT- LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV(XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В	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 централизова

программно-аппаратных средств обеспечения информационной безопасности аудитория №507 (гуманитарный корпус). ***3. учебная аудитория для проведения занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). ***4. учебная аудитория для курсового проектирования (выполнения курсовых работ):***аудитория №613 (гуманитарный корпус). ***5. учебная аудитория для проведения групповых и индивидуальных консультаций:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418		цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт APART 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 APART 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	нного тестировани я БашГУ (Moodle).G N U General Public License.

(гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс		мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 610**	
аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **6.** ***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). **7.** ***помещения для самостоятельной работы:*** читальный		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. **Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507** Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технические средства обработки информации, стенд "Устройство ПК". **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.	

зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **8.*помещение для хранения и профилактического обслуживания учебного оборудования:***аудитория № 523 (гуманитарный корпус).			

Приложение № 1

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

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины **Безопасность критической информационной инфраструктуры** на 9 семестр
___очная_ф/о___

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часов
Учебных часов на контактную работу с преподавателем:	55
лекций	18
практических/ семинарских	18
лабораторных	18
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)	35
из них, предусмотренные на выполнение курсовой работы / курсового проекта	–
Учебных часов на подготовку к зачету (Контроль)	–

Форма контроля
Экзамен 9 семестр

Семестр 9

№	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. Основная проблематика безопасности критической информационной инфраструктуры. Тема: Основные понятия безопасности критических информационной инфраструктуры. Тема: Устойчивость функционирования объектов КИИ относительно компьютерных атак. Тема: Правовое регулирование отношений в области обеспечения безопасности критической информационной инфраструктуры. Тема: Классификация АСУ ТП: требования, параметры, сроки. Тема: Правила категорирования объектов критической информационной инфраструктуры.	2 2 2 2 2	2 2 2 2 2	4	5 5 5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	лабораторная работа, практическая работа, тест
2	Модуль 2. Создание системы защиты информации в критической информационной инфраструктуре. Тема: Разработка модели угроз объектов критической информационной инфраструктуры. Тема: Требования по обеспечению безопасности значимых объектов критической информационной	2 2	2 2	4 4	5 5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы	лабораторная работа, практическая работа, тест

	инфраструктуры. Тема: Выбор мер защиты объекта информатизации критической информационной инфраструктуры. Тема: Формирование технического проекта. Разработка эксплуатационной документации.	2 2	2 2	6	5 5		
Всего часов		18	18	18	35		