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

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

Согласовано:
Председатель УМК института
/ Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина
Комплексная защита объектов информатизации
Б1.В.08

программа специалитета

Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Профиль подготовки
Организация и технологии защиты информации

Квалификация
специалист

Разработчик (составитель)
к.ф.-м.н., доцент
/И.А. Шагапов

Для приема: 2022 г.

Уфа – 2022

Составитель: доцент Шагапов Илдар Ахняфович

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

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета института истории и государственного управления:
_____
_____
_____

Директор _____ А.И. Уразова

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета института истории и государственного управления:
_____
_____
_____

Директор _____ А.И. Уразова

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета института истории и государственного управления:
_____
_____
_____

Директор _____ А.И. Уразова

Дополнения и изменения, внесенные в программу практики, утверждены на заседании ученого совета института истории и государственного управления:
_____
_____
_____

Директор _____ А.И. Уразова

Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций

В результате освоения образовательной программы обучающийся должен овладеть следующими результатами обучения по дисциплине:

Категория (группа) компетенций[1] (при наличии ОПК)	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
	ПК-2 Способен проводить мероприятия по оценке защищенности компьютерных систем и сетей	ПК 2.1 Знать основные мероприятия по оценке защищенности компьютерных систем и сетей	Знает основные мероприятия по оценке защищенности компьютерных систем и сетей
		ПК 2.2 Уметь проводить основные мероприятия по оценке защищенности компьютерных систем и сетей	Умеет проводить основные мероприятия по оценке защищенности компьютерных систем и сетей
		ПК 2.3 Владеть технологией проведения мероприятий по оценке защищенности компьютерных систем и сетей	Владеет технологией проведения мероприятий по оценке защищенности компьютерных систем и сетей

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Комплексная защита объектов информатизации» относится к группе дисциплин обязательной части образовательной программы.

Дисциплина изучается на 5 курсе в А семестре.

Целью освоения дисциплины «Комплексная защита объектов информатизации» является формирование профессиональных компетенций у обучающихся в области комплексной системы защиты информации (КСЗИ), методики и технологии ее организации, принципы и содержание управления системой, методы обеспечения ее надежности.

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 применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности

[1] Указывается только для УК и ОПК (при наличии).

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения	
		«Незачтено»	«Зачтено»
ПК 2.1 Знать основные мероприятия по оценке защищенности компьютерных систем и сетей	Знает основные мероприятия по оценке защищенности компьютерных систем и сетей	Не знает основные мероприятия по оценке защищенности компьютерных систем и сетей	Знает основные нормативные правовые акты, регламентирующие деятельность по комплексной защите информации объектов информатизации
ПК 2.2 Уметь проводить основные мероприятия по оценке защищенности компьютерных систем и сетей	Умеет проводить основные мероприятия по оценке защищенности компьютерных систем и сетей	Не умеет проводить основные мероприятия по оценке защищенности компьютерных систем и сетей	Умеет применять основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по комплексной защите информации объектов информатизации
ПК 2.3 Владеть технологией проведения мероприятий по оценке защищенности компьютерных систем и сетей	Владеет технологией проведения мероприятий по оценке защищенности компьютерных систем и сетей	Не владеет технологией проведения мероприятий по оценке защищенности компьютерных систем и сетей	Владеет технологией применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в сфере профессиональной деятельности

4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
ПК 2.1 Знать основные мероприятия по оценке защищенности компьютерных систем и сетей ПК 2.2 Уметь проводить основные мероприятия по оценке защищенности компьютерных систем и сетей ПК 2.3 Владеть технологией проведения мероприятий по оценке защищенности компьютерных систем и сетей	Знает основные мероприятия по оценке защищенности компьютерных систем и сетей	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2
	Умеет проводить основные мероприятия по оценке защищенности компьютерных систем и сетей	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2
	Владеет технологией проведения мероприятий по оценке защищенности компьютерных систем и сетей	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2

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 зачета:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),
не зачтено – от 0 до 59 рейтинговых баллов).

Рейтинг – план дисциплины

Комплексная защита объектов информатизации

Направление подготовки 10.05.05 БИТвПС

Курс 5, семестр А

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №1	5	1	0	5
3. Практическая работа №2	5	1	0	5
Рубежный контроль				
1. Письменная контрольная работа №1	10	1	0	10
2. Письменная контрольная работа №2	10	1	0	10
1. Лабораторная работа №1	10	1	0	10
Всего				50
Модуль 2.				
Текущий контроль				
1. Аудиторная работа	10	1	1	10
2. Практическая работа №3	5	1	0	5
3. Практическая работа №4	5	1	0	5
Рубежный контроль				
1. Письменная контрольная работа №3	10	1	0	10
2. Письменная контрольная работа №4	10	1	0	10
1. Лабораторная работа №2	10	1	0	10
Всего				50
Поощрительные баллы				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Зачет				

Комплект контрольных работ

Для контроля освоения и/или расширения знаний, умений, владений предусмотрены несколько контрольных работ.

Модуль 1

Письменная контрольная работа №1

Общие вопросы КСЗИ

Вопросы

1. Различные определения КСЗИ

2. Кому, для чего, когда нужна КСЗИ?

3. Кто разрабатывает, создает, эксплуатирует КСЗИ?

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	5
Выполнены пункты 1-3	10
Максимальный балл	10

Письменная контрольная работа №2

Угрозы и уязвимости информационной безопасности

Вопросы

1. Зайти на сайт ФСТЭК, изучить содержание сайта

2. Выбрать на свое усмотрение 3-4 угрозы и 3-4 уязвимости из предложенного банка

3. Изучить их и подготовить краткий отчет.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	5
Выполнены пункты 1-3	10
Максимальный балл	10

Модуль 2

Письменная контрольная работа №3

Оценка и минимизация ущерба

Вопросы

1. Оценка ущерба от нарушителей ИБ.

2. Непредвиденные ситуации и обеспечение безопасности информации.

3. Реагирование на инциденты ИБ.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	5
Выполнены пункты 1-3	10
Максимальный балл	10

Письменная контрольная работа №4

Разработка КСЗИ

Вопросы

1. Принципы организации и этапы разработки КСЗИ
2. Система управления информационной безопасностью предприятия.
3. Требования, предъявляемые к КСЗИ. Этапы разработки КСЗИ

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	5
Выполнены пункты 1-3	10
Максимальный балл	10

Комплект практических заданий

Для самостоятельного освоения и/или расширения знаний, умений, владений предусмотрены несколько практических заданий.

Модуль 1

Типовое практическое задание 1

Модель угроз информационной безопасности

1. Выбрать объект защиты (документ, АРМ, ПК, помещение, АС и т.д.).
2. Собрать необходимую информацию.
3. Построить модель угроз информационной безопасности.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	3
Выполнены пункты 1-3	5
Максимальный балл	5

Типовое практическое задание 2

Модель нарушителя информационной безопасности

1. Выбрать объект защиты (документ, АРМ, ПК, помещение, АС и т.д.).
2. Собрать необходимую информацию.
3. Построить модель нарушителя безопасности.

Методические указания

а. Использовать известные уровни возможностей нарушителя, различные классификации нарушителя.

б. Помнить, для чего строится модель нарушителя.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	3
Выполнены пункты 1-3	5
Максимальный балл	5

Модуль 2

Типовое практическое задание 3

Разработка технического задания (ТЗ) в области информационной безопасности

1. Выбрать вариант для написания ТЗ объект (услуга, работа, разработка, модификация и т..д. в области ИБ)
2. Собрать необходимую информацию.
3. Разработать техническое задание.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-2	3
Выполнены пункты 1-3	5
Максимальный балл	5

Методические указания

а. Изучить ГОСТ по написанию ТЗ и образцы готовых вариантов.
б. Помнить, для чего и для кого разрабатывается ТЗ.

Типовое практическое задание 4

Разработка перечня информации, составляющей коммерческую тайну организации

1. Выбрать (придумать гипотетическую) коммерческую организацию.
2. Изучить деятельность организации.
3. Составить перечень информации (всей), циркулирующей в организации.
4. Провести анализ перечня с фильтрацией информации, имеющей коммерческую ценность для организации.
5. Составить перечень информации, составляющей коммерческую тайну организации

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	3
Выполнены пункты 1-5	5
Максимальный балл	5

Комплект лабораторных работ

Для закрепления на практике знаний, умений, владений предусмотрены несколько лабораторных работ.

Модуль 1

Типовая лабораторная работа 1

Правовая защита информации

1. Для предприятия, выбранного согласно вашему варианту, составить список нормативных правовых актов и стандартов, которыми необходимо руководствоваться при построении комплексной системы защиты информации предприятия. К каждому документу представить комментарий, указывающий обязательный или рекомендательный характер документа, основное содержание документа, область применения документа для рассматриваемого вами предприятия.

   Варианты:

   1. железнодорожная станция;
   6. школа;

7. библиотека;
8. юридическая фирма;
9. фирма по разработке программного обеспечения

2. Составить отчет по работе

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 50%	5
Выполнены пункты 100%	10
Максимальный балл	10

Модуль 2

Типовая лабораторная работа 2

Оценка эффективности системы защиты информации

1. Для коммерческой организации из практической работы №4 разработать систему защиты информации.

3. Выбрать модели оценки экономической эффективности системы защиты.

4. Оценить экономическую эффективность разработанной системы защиты информации выбранной коммерческой организации.

5. Составить отчет по работе.

Критерии оценки

Показатель оценки	Распределение баллов
Выполнены пункты 1-3	5
Выполнены пункты 1-5	10
Максимальный балл	10

Перечень вопросов для зачета:

1. Сущность и задачи комплексной системы защиты информации
2. Основные механизмы информационной безопасности.
3. Основные средства информационной безопасности.
4. Понятие комплексной системы защиты информации.
5. Назначение комплексной системы защиты информации.
6. Принципы построения комплексной системы защиты информации
7. Стратегии защиты информации.
8. Выработка политики безопасности.
9. Основные требования, предъявляемые к комплексной системе защиты информации
10. Определение состава защищаемой информации
11. Методика определения состава защищаемой информации
12. Классификация информации по видам тайны и степеням конфиденциальности
13. Определение объектов защиты
14. Источники, способы и результаты дестабилизирующего воздействия на информацию
15. Определение источников дестабилизирующего воздействия на информацию
16. Методика выявления способов воздействия на информацию
17. Определение причин и условий дестабилизирующего воздействия на информацию
18. Каналы и методы несанкционированного доступа к информации
19. Выявление каналов доступа к информации.

20. Соотношение между каналами и источниками воздействия на информацию
21. Деловая разведка как канал получения информации
22. Модель потенциального нарушителя
23. Факторы, создающие угрозу информационной безопасности.
24. Угрозы безопасности информации.
25. Модели нарушителей безопасности АС.
26. Типовая модель нарушителя безопасности персональных данных в коммерческой организации
27. Моделирование процессов комплексной системы защиты информации
28. Понятие модели объекта.
29. Значение моделирования процессов КСЗИ.
30. Общее содержание работ
31. Этапы разработки
32. Факторы, влияющие на выбор состава КСЗИ
33. Методика выявления состава носителей защищаемой информации
34. Особенности взаимоотношений с контрагентами как объект защиты информации ограниченного доступа
35. Факторы, определяющие необходимость защиты периметра и здания предприятия
36. Особенности помещений как объектов защиты для работы по защите информации
37. Транспортные средства и особенности транспортировки
38. Состав средств обеспечения, подлежащих защите
39. Факторы, создающие угрозу информационной безопасности
40. Угрозы безопасности информации
41. Модели нарушителей безопасности АС
42. Подходы к оценке ущерба от нарушений ИБ
43. Обеспечение безопасности информации в непредвиденных ситуациях
44. Реагирование на инциденты ИБ
45. Резервирование информации и отказоустойчивость
46. Задачи КСЗИ по выявлению угроз и КУИ
47. Особенности защиты речевой информации
48. Механизмы обеспечения безопасности информации
49. Разграничение доступа. Регистрация и аудит
50. Методика выявления нарушителей, тактики их действий и состава интересующей их информации
51. Проектирование системы защиты информации для существующей АС
52. Содержание концепции построения КСЗИ
53. Объекты защиты. Цели и задачи обеспечения безопасности информации
54. Основные принципы построения КСЗИ
55. Меры, методы и средства обеспечения требуемого уровня защищенности информационных ресурсов
56. Первоочередные мероприятия по обеспечению безопасности информации АС организации
57. Общая характеристика задач моделирования КСЗИ
58. Формальные модели безопасности и их анализ
59. Прикладные модели защиты информации в АС
60. Формальное построение модели защиты: пример
61. Характеристика основных стадий создания КСЗИ
62. Назначение и структура технического задания (общие требования к содержанию)
63. Предпроектное обследование, технический проект, рабочий проект.
64. Апробация и ввод в эксплуатацию
65. Распределение функций по защите информации

66. . Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа
67. Подбор и обучение персонала
68. Перечень вопросов ЗИ, требующих документационного закрепления
69. Технология принятия решений в условиях ЧС
70. Факторы, влияющие на принятие решений в условиях ЧС
71. Подготовка мероприятий на случай возникновения ЧС
72. Общая характеристика подходов к оценке эффективности КСЗИ
73. Методы и модели оценки эффективности КСЗИ
74. Показатель уровня защищенности, основанный на экспертных оценках
75. Методы проведения экспертного опроса
76. Экономический подход к оценке эффективности КСЗИ

План лекционных занятий

(16 часов)

Лекция №1

Сущность и задачи комплексной системы защиты информации (2 часа)

1.1. Основные механизмы информационной безопасности. Основные средства информационной безопасности.

1.2. Понятие комплексной системы защиты информации. Назначение комплексной системы защиты информации. Принципы построения комплексной системы защиты информации

1.3. Стратегии защиты информации. Выработка политики безопасности. Основные требования, предъявляемые к комплексной системе защиты информации

Основная литература.

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.

Дополнительная литература.

Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

Лекция №2

Определение состава защищаемой информации (2 часа)

3.1. Методика определения состава защищаемой информации

3.2. Классификация информации по видам тайны и степеням конфиденциальности

3.3. Определение объектов защиты

Основная литература.

Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.

Дополнительная литература.

Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

Лекция №3

Источники, способы и результаты дестабилизирующего воздействия на информацию (2 часа)

4.1. Определение источников дестабилизирующего воздействия на информацию

4.2. Методика выявления способов воздействия на информацию
4.3. Определение причин и условий дестабилизирующего воздействия на информацию

Основная литература.

Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.

Дополнительная литература.

Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

Лекция №4

Каналы и методы несанкционированного доступа к информации (2 часа)

5.1. Выявление каналов доступа к информации.
5.2. Соотношение между каналами и источниками воздействия на информацию
5.3. Деловая разведка как канал получения информации

Основная литература.

Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.

Дополнительная литература.

Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

Лекция №5

Модель нарушителя (2 часа)

6.1. Факторы, создающие угрозу информационной безопасности. Угрозы безопасности информации.
6.2. Модели нарушителей безопасности АС.
6.3. Типовая модель нарушителя безопасности персональных данных в коммерческой организации

Основная литература.

Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

Дополнительная литература.

Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.

Третьякова Т.И. Типовая модель нарушителя безопасности персональных данных в коммерческой организации (статья в журнале, прилагается вариант в гугл-диске)

Лекция №6

Защита информации и персонал (2 часа)

6.1 Распределение функций по защите информации
6.2 Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа
6.2 Подбор и обучение персонала

Основная литература.

Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. посо-

бие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

Дополнительная литература.

Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.

Третьякова Т.И. Типовая модель нарушителя безопасности персональных данных в коммерческой организации (статья в журнале, прилагается вариант в гугл-диске)

Лекция №7

Защита информации в условиях ЧС (2 часа)

7 Технология принятия решений в условиях ЧС

8 Факторы, влияющие на принятие решений в условиях ЧС

9 Подготовка мероприятий на случай возникновения ЧС

Основная литература.

Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

Дополнительная литература.

Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.

Третьякова Т.И. Типовая модель нарушителя безопасности персональных данных в коммерческой организации (статья в журнале, прилагается вариант в гугл-диске)

Лекция №8

Общая характеристика подходов к оценке эффективности КСЗИ (2 часа)

9.1 Методы и модели оценки эффективности КСЗИ

9.2 Показатель уровня защищенности, основанный на экспертных оценках

9.3 Методы проведения экспертного опроса

9.4 Экономический подход к оценке эффективности КСЗИ

Основная литература.

Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

Дополнительная литература.

Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.

Планы семинарских занятий

(32 часа)

Семинар №1-2

Сущность и задачи комплексной системы защиты информации (4 часа)

1. Основные механизмы информационной безопасности. Основные средства информационной безопасности.
2. Понятие комплексной системы защиты информации. Назначение комплексной системы защиты информации. Принципы построения комплексной системы защиты информации
3. Стратегии защиты информации. Выработка политики безопасности.

4. Основные требования, предъявляемые к комплексной системе защиты информации

Основная литература.

Конеев И.Р. Беляев А.В. Информационная безопасность предприятия, СПб, 2003, 752 с.

Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.

Дополнительная литература.

Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

Семинар №3-4

Определение состава защищаемой информации (4 часа)

1. Защищаемая информация
2. Методика определения состава защищаемой информации
3. Классификация информации по видам тайны и степеням конфиденциальности
4. Определение объектов защиты

Основная литература.

Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.

Дополнительная литература.

Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

Семинар №5-6

Источники, способы и результаты дестабилизирующего воздействия на информацию (4 часа)

1. Дестабилизирующее воздействие на информацию
2. Определение источников дестабилизирующего воздействия на информацию
3. Методика выявления способов воздействия на информацию
4. Определение причин и условий дестабилизирующего воздействия на информацию

Основная литература.

Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.

Дополнительная литература.

Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

Семинар №7-8

Каналы и методы несанкционированного доступа к информации (4 часа)

1. Каналы доступа к информации
2. Выявление каналов доступа к информации.
3. Соотношение между каналами и источниками воздействия на информацию
4. Деловая разведка как канал получения информации

Основная литература.

Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.

Дополнительная литература.

Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

Семинар №9-10

Модель нарушителя (4 часа)

1. Факторы, создающие угрозу информационной безопасности.
2. Угрозы безопасности информации.
3. Модели нарушителей безопасности АС.
4. Типовая модель нарушителя безопасности персональных данных в коммерческой организации

Основная литература.

Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

Дополнительная литература.

Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.

Третьякова Т.И. Типовая модель нарушителя безопасности персональных данных в коммерческой организации (статья в журнале, прилагается вариант в гугл-диске)

Семинар №11-12

Защита информации и персонал (4 часа)

1. Распределение функций по защите информации
2. Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа
3. Подбор персонала
4. Обучение персонала

Основная литература.

Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

Дополнительная литература.

Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.

Третьякова Т.И. Типовая модель нарушителя безопасности персональных данных в коммерческой организации (статья в журнале, прилагается вариант в гугл-диске)

Семинар №13-14

Защита информации в условиях ЧС (4 часа)

1. ЧС и защита информации
2. Технология принятия решений в условиях ЧС
3. Факторы, влияющие на принятие решений в условиях ЧС
4. Подготовка мероприятий на случай возникновения ЧС

Основная литература.

Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский

центр «Академия», 2009. — 416 с.

Дополнительная литература.

Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.

Третьякова Т.И. Типовая модель нарушителя безопасности персональных данных в коммерческой организации (статья в журнале, прилагается вариант в гугл-диске)

Семинар №15-16

Общая характеристика подходов к оценке эффективности КСЗИ (4 часа)

1. Методы и модели оценки эффективности КСЗИ
2. Показатель уровня защищенности, основанный на экспертных оценках
3. Методы проведения экспертного опроса
4. Экономический подход к оценке эффективности КСЗИ

Основная литература.

Грибунин В. Г. Комплексная система защиты информации на предприятии : учеб. пособие для студ. высш. учеб. заведений /В. Г. Грибунин, В.В.Чудовский. — М. : Издательский центр «Академия», 2009. — 416 с.

Дополнительная литература.

Гришина Н. В. Организация комплексной системы защиты информации. — М.: Гелиос АРВ, 2007. — 256 с.

Критерии оценки (в баллах) *(должны строго соответствовать рейтинг плану по макс. и мин. колич. баллов и только для тех, кто учится с использованием модульно-рейтинговой системы обучения и оценки успеваемости студентов):*

- 0,55 баллов выставляется студенту, если выполнил задание на 100%

- 0,36 баллов выставляется студенту, если выполнил задание на 75%

- 0,2 баллов выставляется студенту, если выполнил задание на 50%

- 0 баллов выставляется студенту, если не выполнил задание

5. Учебно-методическое и информационное обеспечение дисциплины

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

1. Аверченков, В.И. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=93356
2. Плашенков, В. Обеспечение безопасности бизнеса промышленных предприятий: теория и практика : учебное пособие / В. Плашенков ; науч. ред. А.Н. Зуев ; Министерство образования и науки Российской Федерации, Федеральное государственное бюджетное образовательное учреждение высшего профессионального образования «ЧЕРЕПОВЕЦКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ», Институт информационных технологий. - Череповец : Издательство ЧГУ, 2014. - 331 с. : ил., табл. - Библиогр. в кн. - ISBN 978-5-85341-634-5 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=434840
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

Дополнительная литература

4. Сердюк, В.А. Организация и технологии защиты информации: обнаружение и предотвращение информационных атак в автоматизированных системах предприятий: учебное пособие / В.А. Сердюк ; Высшая Школа Экономики Национальный Исследовательский Университет. - Москва : Издательский дом Высшей школы экономики, 2015. - 574 с. : ил. - Библиогр. в кн. - ISBN 978-5-7598-0698-1 ; То же [Электронный ресурс]. - URL: http://biblioclub.ru/index.php?page=book&id=440285
5. Больбат, Е.П. ПРООЕКТИРОВАНИЕ КОМПЛЕКСНОЙ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ НА ПРЕДПРИЯТИИ (КОНФИДЕНЦИАЛЬНАЯ ИНФОРМАЦИЯ). [Электронный ресурс] — Электрон. дан. // Вестник научного общества студентов, аспирантов и молодых ученых. — 2015. — № 3. — С. 21-25. — Режим доступа: http://e.lanbook.com/journal/issue/294140 — Загл. с экрана.
6. Масалков, А.С. Особенности киберпреступлений: инструменты нападения и защиты информации [Электронный ресурс] / А.С. Масалков. — Электрон. дан. — Москва : ДМК Пресс, 2018. — 226 с. — Режим доступа: https://e.lanbook.com/book/105842. — Загл. с экрана.
7. Семь безопасных информационных технологий [Электронный ресурс] : учебник / А.В. Барабанов [и др.] ; под ред. Маркова А.С.. — Электрон. дан. — Москва : ДМК Пресс, 2017. — 224 с. — Режим доступа: https://e.lanbook.com/book/97352. — Загл. с экрана.
8. Бойченко, О.В. ПРОБЛЕМАТИКА КОМПЛЕКСНОЙ ОЦЕНКИ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ [Электронный ресурс] / О.В. Бойченко, Б.В. Белименко. // Ученые записки Крымского федерального университета им. В.И. Вернадского. Экономика и управление. — Электрон. дан. — 2015. — № 1. — С. 27-31. — Режим доступа: https://e.lanbook.com/journal/issue/299849. — Загл. с экрана.

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

1. Справочная правовая система «КонсультантПлюс» – http://www.consultant-plus.ru.
2. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
3. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
4. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
5. www.fstec.ru –сайт ФСТЭК России
6. www.fsb.ru – сайт ФСБ России
7. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. http://univertv.ru/video/matematika/ – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);
9. www.newlibrary.ru – Новая электронная библиотека;
10. www. edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.
13. 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.

14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
15. Система централизованного тестирования БашГУ (Moodle).GNU General Public License

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*****:** Лаборатория полигон технической защиты информации № 508 (гуманитарный корпус), компьютерный класс, аудитория 404 (гуманитарный корпус), аудитория 420 (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***	Лекции, практические занятия, лабораторные занятия, 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 коротк-кофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTEL-Corei3-4150/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., Двухполосный 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 на-	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.

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). **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:*** читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус). **7.*помещение для хранения и профилактического обслуживания учебного оборудования:*** аудитория № 523 (гуманитарный корпус).		стенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 610** Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м. **Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Аудитория 402 читальный зал библиотеки** Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбини-	

		рованные. **Лаборатория полигон технической защиты информации № 508** Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технической защиты информации, комплекс мониторинга WiFi сетей "Зодиак II", универсальный ком-плект инструментов для проведения работ по специальным провер-кам и специальным обследованиям Калейдоскоп-П2, многофункциональный поисковый прибор ST-031M "Пиранья", нелинейный локатор «Лорнет», анализатор электромагнитного поля "Кордон". **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.	

Приложение 1

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

Содержание рабочей программы
дисциплины

Вид работы	**Объем дисциплины**
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часов
Учебных часов на контактную работу с преподавателем:	48
лекций	16
практических/ семинарских	32
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	60
Учебных часов на подготовку к зачету	

Форма контроля:
Зачет А семестр

№	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР / Сем	ЛР	СРС		
1	2	3	4	5	6	7	8
1	Сущность и задачи комплексной системы защиты информации Основные механизмы информационной безопасности. Основные средства информационной безопасности. Понятие комплексной системы защиты информации. Назначение комплексной системы защиты информации. Принципы построения комплексной системы защиты информации Стратегии защиты информации. Выработка политики безопасности. Основные требования, предъявляемые к комплексной системе защиты информации	2	4		8	Изучить вопросы определения несанкционированного доступа к защищаемой информации	Письменная контрольная работа Практическое задание Лабораторная работа
2	Определение состава защищаемой информации Методика определения состава защищаемой информации Классификация информации по видам тайны и степеням конфиденциальности Определение объектов защиты	2	4		8	Изучить возможности несанкционированного доступа к защищаемой информации	Письменная контрольная работа Практическое задание Лабораторная работа
3	Источники, способы и результаты дестабилизирующего воздействия на информацию Определение источников дестабилизирующего воздействия на информацию Методика выявления способов воздействия на информацию Определение причин и условий дес-	2	4		8	Изучить актуальные вопросы построения КСЗИ	Письменная контрольная работа Практическое задание Лабораторная работа

	табилизирующего воздействия на информацию						
4	Каналы и методы несанкционированного доступа к информации) Выявление каналов доступа к информации. Соотношение между каналами и источниками воздействия на информацию Деловая разведка как канал получения информации	2	4		8	Изучить вопросы оправданности построения КСЗИ	Письменная контрольная работа Практическое задание Лабораторная работа
5	Модель нарушителя Факторы, создающие угрозу информационной безопасности. Угрозы безопасности информации. Модели нарушителей безопасности АС. Типовая модель нарушителя безопасности персональных данных в коммерческой организации	2	4		8	Изучить зарубежный опыт подходов к оценке эффективности КСЗИ	Письменная контрольная работа Практическое задание Лабораторная работа
6	Защита информации и персонал Распределение функций по защите информации Обеспечение взаимодействия между субъектами, защищающими и использующими информацию ограниченного доступа Подбор и обучение персонала	2	4		8	Изучить советский опыт подходов к оценке эффективности КСЗИ	Письменная контрольная работа Практическое задание Лабораторная работа
7	Защита информации в условиях ЧС Технология принятия решений в условиях ЧС Факторы, влияющие на принятие решений в условиях ЧС Подготовка мероприятий на случай возникновения ЧС	2	4		8	Изучить правовые аспекты защиты информации в условиях чрезвычайных ситуаций. Оценить эффективность правовых аспектов защиты информации в условиях чрезвычайных ситуаций	Письменная контрольная работа Практическое задание Лабораторная работа
8	Общая характеристика подходов к оценке эффективности КСЗИ Методы и модели оценки эффективности КСЗИ Показатель уровня защищенности, основанный на экспертных оценках	2	4		4	Сравнить отечественный и зарубежный опыт подходов к оценке эффективности КСЗИ	Письменная контрольная работа Практическое задание Лабораторная работа

	Методы проведения экспертного опроса Экономический подход к оценке эффективности КСЗИ						
	Итого	16	32		60		