


МИНОБРНАУКИ РОССИИ
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 (МОДУЛЯ)

Дисциплина
Основы комплексной защиты объектов информатизации

Обязательная часть
программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

Профиль подготовки
Организация и технология защиты информации
(в системе государственного и муниципального управления)

Квалификация
бакалавр

Разработчик (составитель)
к.ф.-м.н., доцент



/И.А. Шагапов

Для приема: 2021 г.

Уфа – 2021

Составитель: доцент Шагапов Илдар Ахняфович

Рабочая программа дисциплины утверждена на заседании кафедры, протокол № 8 от «24» февраля 2021 г.

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	7
5. Учебно-методическое и информационное обеспечение дисциплины	21
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	21
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы	22
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	23

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 (при наличии ОПК)	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
	ОПК-5 Способен применять нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по защите информации в сфере профессиональной деятельности	ОПК 5.4 Знать основные нормативные правовые акты, регламентирующие деятельность по комплексной защите информации объектов информатизации	Знает основные нормативные правовые акты, регламентирующие деятельность по комплексной защите информации объектов информатизации
		ОПК 5.5 Уметь применять основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по комплексной защите информации объектов информатизации	Умеет применять основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по комплексной защите информации объектов информатизации
		ОПК 5.6 Владеть технологией применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в сфере профессиональной деятельности	Владеет технологией применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в сфере профессиональной деятельности
	ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ОПК 8.1 Знать методы подбора, изучения и обобщения научно-технической литературы по комплексной защите информации объектов информатизации	Знает методы подбора, изучения и обобщения научно-технической литературы по комплексной защите информации объектов информатизации
		ОПК 8.2 Уметь подбирать, изучать и обобщать научно-техническую литературу, нормативные и методические документы в целях решения задач по комплексной защите информации объектов информатизации	Умеет подбирать, изучать и обобщать научно-техническую литературу, нормативные и методические документы в целях решения задач по комплексной защите информации объектов информатизации
		ОПК 8.3 Владеть технологией подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	Владеет технологией подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Основы комплексной защиты объектов информатизации» относится к группе дисциплин обязательной части образовательной программы.

Дисциплина изучается на 4 курсе в 7 семестре.

Целью освоения дисциплины «Основы комплексной защиты 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

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения			
		«Неудовлетворительно»	«Удовлетворительно»	«Хорошо»	«Отлично»
ОПК 5.4 Знать основные нормативные правовые акты, регламентирующие деятельность по комплексной защите информации объектов информатизации	Знает основные нормативные правовые акты, регламентирующие деятельность по комплексной защите информации объектов информатизации	Не знает основные нормативные правовые акты, регламентирующие деятельность по комплексной защите информации объектов информатизации	Понимает важность знаний по основным нормативным правовым актам, регламентирующим деятельность по комплексной защите информации объектов информатизации	Частично знает основные нормативные правовые акты, регламентирующие деятельность по комплексной защите информации объектов информатизации, но делает ошибки	Знает основные нормативные правовые акты, регламентирующие деятельность по комплексной защите информации объектов информатизации
ОПК 5.5 Уметь применять основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по комплексной защите информации объектов информатизации	Умеет применять основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по комплексной защите информации объектов информатизации	Не умеет применять основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по комплексной защите информации объектов информатизации	Умеет применять некоторые нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по комплексной защите информации объектов информатизации	Частично умеет применять основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по комплексной защите информации объектов информатизации, но делает ошибки	Умеет применять основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по комплексной защите информации объектов информатизации

ОПК 5.6 Владеть технологией применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в сфере профессиональной деятельности	Владеет технологией применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в сфере профессиональной деятельности	Не владеет технологией применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в сфере профессиональной деятельности	Владеет технологией применения некоторых нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в сфере профессиональной деятельности	Частично владеет технологией применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в сфере профессиональной деятельности, но делает ошибки	Владеет технологией применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в сфере профессиональной деятельности
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания результатов обучения			
		«Неудовлетворительно»	«Удовлетворительно»	«Хорошо»	«Отлично»
ОПК 8.1 Знать методы подбора, изучения и обобщения научнотехнической литературы по комплексной защите информации объектов информатизации	Знает методы подбора, изучения и обобщения научнотехнической литературы по комплексной защите информации объектов информатизации	Не знает методы подбора, изучения и обобщения научнотехнической литературы по комплексной защите информации объектов информатизации	Знает методы подбора, изучения и обобщения научнотехнической литературы по комплексной защите информации объектов информатизации	Фрагментарно знает методы подбора, изучения и обобщения научнотехнической литературы по комплексной защите информации объектов информатизации	Знает методы подбора, изучения и обобщения научнотехнической литературы по комплексной защите информации объектов информатизации
ОПК 8.2 Уметь подбирать, изучать и обобщать научнотехническую литературу, нормативные и методические документы в целях решения задач по комплексной защите информации объектов информатизации	Умеет подбирать, изучать и обобщать научнотехническую литературу, нормативные и методические документы в целях решения задач по комплексной защите информации объектов информатизации	Не умеет подбирать, изучать и обобщать научнотехническую литературу, нормативные и методические документы в целях решения задач по комплексной защите информации объектов информатизации	Умеет подбирать, изучать и обобщать нормативные и методические документы в целях решения задач по комплексной защите информации объектов информатизации	Умеет подбирать, изучать и обобщать некоторые научнотехническую литературу, нормативные и методические документы в целях решения задач по комплексной защите информации объектов информатизации	Умеет подбирать, изучать и обобщать научнотехническую литературу, нормативные и методические документы в целях решения задач по комплексной защите информации объектов информатизации
ОПК 8.3 Владеть технологией подбора, изучения и обобщения	Владеет технологией подбора, изучения и обобщения научно-	Не владеет технологией подбора, изучения и обобщения научно-	Владеет основами технологии подбора, изучения и обобщения нормативных	Частично владеет технологией подбора, изучения и обобщения	Владеет технологией подбора, изучения и обобщения научно-

научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	ратуры, нормативных и методических документов в целях решения задач профессиональной деятельности	и методических документов в целях решения задач профессиональной деятельности	научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	технической литературы, нормативных и методических документов в целях решения задач 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
<p>ОПК 5.4 Знать основные нормативные правовые акты, регламентирующие деятельность по комплексной защите информации объектов информатизации</p> <p>ОПК 5.5 Уметь применять основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по комплексной защите информации объектов информатизации</p> <p>ОПК 5.6 Владеть технологией применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в сфере профессиональной деятельности</p>	Знает основные нормативные правовые акты, регламентирующие деятельность по комплексной защите информации объектов информатизации	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2
	Умеет применять основные нормативные правовые акты, нормативные и методические документы, регламентирующие деятельность по комплексной защите информации объектов информатизации	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2
	Владеет технологией применения нормативных правовых актов, нормативных и методических документов, регламентирующих деятельность по защите информации в сфере профессиональной деятельности	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Оценочные средства
<p>ОПК 8.1 Знать методы подбора, изучения и обобщения научно-технической литературы по комплексной защите информации объектов информатизации</p> <p>ОПК 8.2 Уметь подбирать, изучать и обобщать научно-техническую литературу, нормативные и методические документы в целях решения задач по комплексной защите информации объектов информатизации</p> <p>ОПК 8.3 Владеть технологией</p>	Знает методы подбора, изучения и обобщения научно-технической литературы по комплексной защите информации объектов информатизации	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2
	Умеет подбирать, изучать и обобщать научно-техническую литературу, нормативные и методические документы в целях решения задач по комплексной защите информации объектов информатизации	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2
	Владеет технологией подбора, изучения и обобщения научно-технической литературы, нормативных и методических докумен-	Письменная контрольная работа 1,2,3,4 Практическое задание 1,2,3,4 Лабораторная работа 1,2

гией подбора, изучения и обобщения научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности	тов в целях решения задач профессиональной деятельности	
-------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------	--

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».

Рейтинг – план дисциплины

Основы комплексной защиты объектов информатизации

Направление подготовки 10.03.01 ИБ

Курс 4, семестр 7

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	4	1	0	4
2. Письменная контрольная работа №2	4	1	0	4
1. Лабораторная работа №1	7	1	0	7
Всего				35
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	4	1	0	4
2. Письменная контрольная работа №4	4	1	0	4
1. Лабораторная работа №2	7	1	0	7
Всего				35

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				
Экзамен				30

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	2
Выполнены пункты 1-3	4
Максимальный балл	4

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	2
Выполнены пункты 1-3	4
Максимальный балл	4

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	2
Выполнены пункты 1-3	4
Максимальный балл	4

**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	2
Выполнены пункты 1-3	4
Максимальный балл	4

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%	3
Выполнены пункты 100%	7
Максимальный балл	7

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	3
Выполнены пункты 1-5	7
Максимальный балл	7

Экзаменационные билеты¹

Структура экзаменационного билета: экзаменационный билет содержит 2 теоретиче-

¹Если итоговой формой контроля является зачет, то приводится перечень вопросов и критерии оценки для зачета (с учетом наличия/отсутствия модульно–рейтинговой системы оценок).

ских вопроса.

Перечень вопросов для экзамена:

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. Аprobация 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

Образец экзаменационного билета:

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

Направление подготовки 10.03.01 «Информационная безопасность»

Дисциплина: Основы комплексной защиты объектов информатизации

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 2

1. Назначение комплексной системы защиты информации.
 2. Основные принципы построения КСЗИ
- Зав. кафедрой УИБ

А.С. Исмагилова

Кафедра управления информационной безопасностью

Критерии оценки (в баллах):

- **25-30 баллов** выставляется студенту, если студент дал полные, развернутые ответы на все теоретические вопросы билета, продемонстрировал знание функциональных возможностей, терминологии, основных элементов, умение применять теоретические знания при выполнении практических заданий. Студент без затруднений ответил на все дополнительные вопросы. Практическая часть работы выполнена полностью без неточностей и ошибок;

- **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. При выполнении практической части работы допущены несущественные ошибки;

- **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. Студент не решил задачу или при решении допущены грубые ошибки;

- **0-10 баллов** выставляется студенту, если он отказался от ответа или не смог ответить на вопросы билета, 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.

План лекционных занятий

(18 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. 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 №7

Контрольные мероприятия в КСЗИ (2 часа)

7 Основы подготовки и принятия решений при планировании

8 Методы сбора, обработки и изучения информации, необходимой для планирования

9 Проведение контрольных мероприятий в КСЗИ

10 Цель проведения контрольных мероприятий в КСЗИ

11 Анализ и использование результатов проведения контрольных мероприятий

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

Защита информации в условиях ЧС (2 часа)

12 Технология принятия решений в условиях ЧС

13 Факторы, влияющие на принятие решений в условиях ЧС

14 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 ком-

мерческой организации (статья в журнале, прилагается вариант в гугл-диске)

Лекция №9

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

(36 часов)

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 (2 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

Контрольные мероприятия в КСЗИ (4 часа)

1. Основы подготовки и принятия решений при планировании
2. Методы сбора, обработки и изучения информации, необходимой для планирования
3. Проведение контрольных мероприятий в КСЗИ
4. Цель проведения контрольных мероприятий в КСЗИ
5. Анализ и использование результатов проведения контрольных мероприятий

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

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 №17-18

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. Большат, Е.П. ПРОЕКТИРОВАНИЕ 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	
<p>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).</p> <p>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).</p> <p>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).</p> <p>4. учебная аудитория для проведения групповых и индивидуальных консультаций: аудитория № 403 (гуманитарный корпус), аудитория № 415 (гу-</p>	<p>Лекции, практические занятия, лабораторные занятия, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация</p>	<p>Аудитория № 403 Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия.</p> <p>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 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 HDMIC-MPRO 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.</p> <p>Аудитория № 413 Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p>Аудитория № 415 Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p>Аудитория № 416 Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт.</p> <p>Аудитория № 418 Учебная мебель, доска, Экран настенный Lumien Master Piktura 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт.</p> <p>Аудитория № 419 Учебная мебель, Проектор Optoma</p>	<p>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.</p> <p>2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.</p> <p>3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License. Лицензии бессрочные.</p>

<p>манитарный 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).</p> <p>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).</p> <p>6. помещения для самостоятельной работы: читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус).</p> <p>7.помещение для хранения и профилактического обслуживания учебного оборудования: аудитория № 523 (гуманитарный корпус).</p>		<p>Ex542 i – 1 шт., Экран настенный Dinon – 1 шт.</p> <p>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, профессиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CМPRO 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.</p> <p>Аудитория № 516 Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.</p> <p>Аудитория № 509 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 608 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>Аудитория № 609 Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p>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.</p> <p>Аудитория № 613 Учебная мебель, доска, моноблок стационарный – 15 шт.</p> <p>Компьютерный класс аудитория № 420 Учебная мебель, моноблоки стационарные 15 шт.</p> <p>Компьютерный класс аудитория № 404 Учебная мебель, компьютеры -15 штук.</p> <p>Аудитория 402 читальный зал библиотеки Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные.</p> <p>Лаборатория полигон технической защиты информации № 508 Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекцион-</p>	
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

		<p>ная, плакаты с тематикой технической защиты информации, комплекс мониторинга WiFi сетей "Зодиак II", универсальный ком-плект инструментов для проведения работ по специальным проверкам и специальным обследованиям Калейдоскоп-П2, многофункциональный поисковый прибор ST-031M "Пиранья", нелинейный локатор «Лорнет», анализатор электромагнитного поля "Кордон".</p> <p>Аудитория № 523</p> <p>Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.</p>	
--	--	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--

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:	55
лекций	18
практических/ семинарских	36
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
Учебных часов на самостоятельную работу обучающихся (СР)	16,8
Учебных часов на подготовку к экзамену	36

Форма контроля:
 экзамен 7 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		2	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		2	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 де-	2	4		2	Изучить актуальные вопросы построения КСЗИ	Письменная контрольная работа Практическое задание Лабораторная работа

	стабилизирующего 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		2	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		2	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		2	Изучить советский опыт подходов к оценке эффективности КСЗИ Письменная контрольная работа Практическое задание Лабораторная работа
7	Контрольные мероприятия в КСЗИ Основы подготовки и принятия решений при планировании Методы сбора, обработки и изучения информации, необходимой для планирования Проведение контрольных мероприятий в КСЗИ Цель проведения контрольных мероприятий в КСЗИ Анализ и использование результатов проведения контрольных мероприятий	2	4		2	Изучить российский опыт подходов к оценке эффективности КСЗИ Письменная контрольная работа Практическое задание Лабораторная работа

8	<p>Защита информации в условиях ЧС</p> <p>Технология принятия решений в условиях ЧС</p> <p>Факторы, влияющие на принятие решений в условиях ЧС</p> <p>Подготовка мероприятий на случай возникновения ЧС</p>	2	4		2	<p>Изучить правовые аспекты защиты информации в условиях чрезвычайных ситуаций. Оценить эффективность правовых аспектов защиты информации в условиях чрезвычайных ситуаций</p>	<p>Письменная контрольная работа</p> <p>Практическое задание</p> <p>Лабораторная работа</p>
9	<p>Общая характеристика подходов к оценке эффективности КСЗИ</p> <p>Методы и модели оценки эффективности КСЗИ</p> <p>Показатель уровня защищенности, основанный на экспертных оценках</p> <p>Методы проведения экспертного опроса</p> <p>Экономический подход к оценке эффективности КСЗИ</p>	2	4		1	<p>Сравнить отечественный и зарубежный опыт подходов к оценке эффективности КСЗИ</p>	<p>Письменная контрольная работа</p> <p>Практическое задание</p> <p>Лабораторная работа</p>
	Итого	18	36		17		

