


МИНОБРНАУКИ РОССИИ
ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
ФАКУЛЬТЕТ БАШКИРСКОЙ ФИЛОЛОГИИ, ВОСТОКОВЕДЕНИЯ И ЖУРНАЛИСТИКИ

Утверждено:
на заседании кафедры
протокол №4 от 13 января 2022 г.

И.о.зав. кафедрой  /Мустафина Р.Д.

Согласовано:
Председатель УМК факультета
башкирской филологии, востоковедения и
журналистики

 / Гареева Г.Н.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Дисциплина Информационная безопасность


Часть, формируемая участниками образовательных отношений

программа бакалавриата

Направление подготовки
42.03.02 Журналистика

Направленность (профиль) подготовки
Корреспондент средств массовой информации на башкирском языке

Квалификация
Бакалавр

Разработчик (составитель) Доцент, канд.филол.наук	 Р.Д.Мустафина
--	--

Для приема: 2022

Уфа — 2022 г.

Составитель: к.ф.н., доц. Р.Д.Мустафина

Рабочая программа дисциплины утверждена на заседании кафедры протокол № 4
от «3 января 2022 г.

И.о.зав. кафедрой



Мустафина Р.Д.

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	4
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	6
4.2. Типовые контрольные задания или иные материалы, необходимые для оценивания результатов обучения по дисциплине, соотнесенных с установленными в образовательной программе индикаторами достижения компетенций. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине	8
5. Учебно-методическое и информационное обеспечение дисциплины	16
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	16
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины, включая профессиональные базы данных и информационные справочные системы	16
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	17

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

В результате освоения образовательной программы обучающийся должен достичь следующих результатов обучения

Категория (группа компетенций)	Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине
1. Профессиональные компетенции	ПК-5: способен к анализу, оцениванию и редактированию медиатекстов, приведению их в соответствие с нормами, стандартами, форматами, стилями, технологическими требованиями, принятыми в СМИ разных типов	ИПК-5.1. Знает: принципы редактирования медиатекстов	Знать принципы редактирования медиатекстов
		ИПК-5.2. Умеет: анализировать и оценивать медиатексты с учетом требований, принятых в СМИ разных типов	Уметь анализировать и оценивать медиатексты с учетом требований, принятых в СМИ разных типов
		ИПК-5.3. Владеет: навыками редактирования медиатекстов разных типов	Владеть навыками редактирования медиатекстов разных типов

2.Цель и место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» относится к части, формируемой участниками образовательных отношений

Дисциплина изучается на 4 курсе в 8 семестре очной формы обучения.

Цель изучения дисциплины — познакомить с принципами обеспечения информационной безопасности, подходами к анализу угроз информационной инфраструктуры как самого журналиста, так и всей редакции; освоение дисциплинарных компетенций для решения задач защиты информации в информационных системах, а также формирование фундаментальных знаний в области информационной безопасности.

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

Код и формулировка компетенции: ПК-5: Способен к анализу, оцениванию и редактированию медиатекстов, приведению их в соответствие с нормами, стандартами, форматами, стилями, технологическими требованиями, принятыми в СМИ разных типов.

Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине	Критерии оценивания	
		«Не зачтено»	«Зачтено»
ИПК-5.1. Знает: принципы редактирования медиатекстов	Знать: принципы редактирования медиатекстов	Не знает или знает недостаточно принципы редактирования медиатекстов	Знает принципы редактирования медиатекстов
ИПК-5.2. Умеет: анализировать и оценивать медиатексты с учетом требований, принятых в СМИ разных типов.	Уметь: анализировать и оценивать медиатексты с учетом требований, принятых в СМИ разных типов.	Не умеет или умеет недостаточно анализировать и оценивать медиатексты с учетом требований, принятых в СМИ разных типов	Умеет анализировать и оценивать медиатексты с учетом требований, принятых в СМИ разных типов
ИПК-5.3. Владеет: навыками редактирования медиатекстов разных типов	Владеть: навыками редактирования медиатекстов разных типов	Не владеет или владеет недостаточно навыками редактирования медиатекстов разных типов	Владеет навыками редактирования медиатекстов разных типов

Критериями оценивания 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».

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
--	-----------------------------------	--------------------

ИПК-5.1. Знает: принципы редактирования медиатекстов	Знать принципы редактирования медиатекстов	Индивидуальный опрос Доклад Практическое задание
ИПК-5.2. Умеет: анализировать и оценивать медиатексты с учетом требований, принятых в СМИ разных типов	Уметь анализировать и оценивать медиатексты с учетом требований, принятых в СМИ разных типов	Индивидуальный опрос Доклад Практическое задание
ИПК-5.3. Владеет: навыками редактирования медиатекстов разных типов	Владеть навыками редактирования медиатекстов разных типов	Индивидуальный опрос Доклад Практическое задание

Рейтинг – план дисциплины
Информационная безопасность

направление/специальность 42.03.02 Журналистика
курс 4, семестр 8

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1				
Текущий контроль				20
1. Индивидуальный опрос	5	2	1	10
2. Доклад	10	1	1	10
Рубежный контроль				30
1. Практическое задание	15	1	1	30
Модуль 2				
Текущий контроль				20
1. Индивидуальный опрос	5	2	1	10
2. Доклад	10	1	1	10
Рубежный контроль				30
1. Практическое задание	15	1	1	30
Итоговый контроль				
зачет			0	0
Поощрительные баллы				

1. Студенческая олимпиада			1	5
2. Публикация статей			1	5
Итого				110

Примерные вопросы для индивидуальных опросов

Индивидуальный опрос проводится после изучения теоретического материала модуля с целью выяснения наиболее сложных вопросов, степени усвоения учебного теоретического материала. Этот метод контроля применяется для оценки знания одного студента или группы.

Вопрос задается всей группе, затем необходима небольшая пауза для того, чтобы все студенты приготовились к ответу, а вызывают для ответа конкретного студента. Чтобы группа слушала ответ своего товарища, студентам предлагается оценить полноту и глубину ответа в виде рецензирования. Оценивается ответ не только отвечающего студента, но и тех, кто участвовал в обсуждении.

Расскажите про понятие национальной безопасности.

1. Информационная безопасность в системе национальной безопасности Российской Федерации.
2. Государственная информационная политика.
3. Основные понятия, общеметодологические принципы теории информационной безопасности.
4. Анализ угроз информационной безопасности.
5. Проблемы информационных войн.
6. Проблемы региональной информационной безопасности.
7. Виды информации ограниченного доступа.
8. Методы нарушения конфиденциальности, целостности и доступности информации.
9. Причины, виды, каналы утечки и искажения информации.
10. Формальные модели безопасности.
11. Способы и средства обеспечения информационной безопасности.
12. Критерии оценки защищенности информационных систем.

Высшая оценка – 5 баллов

Критерии оценки в баллах:

5 баллов выставляется студенту, если: 1) демонстрирует умение анализировать и теоретически оценивать эмпирические факты; 2) он устанавливает междисциплинарные связи; 3) обнаруживает аналитический подход в освещении разных концепций; 4); приводит убедительные примеры из практики работы журналистов; 5) обосновывает свою точку зрения.

4 балла выставляется студенту, если выполнено всего 4 из вышеуказанных условий;

3 балла выставляется студенту, если выполнено всего 3 из вышеуказанных условий;

2 балла выставляется студенту, если проявил неудовлетворительное владение материалом работы и не смог ответить на большинство поставленных вопросов по теме. Студент продемонстрировал недостаточный уровень владения умениями и навыками при решении профессиональных задач в рамках усвоенного учебного материала;

1 балл выставляется студенту, если нет понимания вопроса, допущены ошибки в определении понятий, использовании терминологии, не смог ответить ни на один поставленный вопрос по теме. Студент продемонстрировал полное отсутствие владения

умениями и навыками при решении профессиональных задач в рамках усвоенного учебного материала

Темы для докладов

Доклад рассчитан на 15 минут. Структурно он должен состоять из трех частей: вводной, основной и заключительной. Во вводной части доклада обычно раскрывается научно-практическое значение темы сообщения, перечисляются основные вопросы содержания доклада. В основной части излагается материал, приводятся точки зрения на выдвинутую проблему. Студенту желательно высказать собственное мнение по излагаемой теме. В заключительной части доклада делаются краткое обобщение выступления и выводы.

1. Угрозы информационной безопасности и факторы, воздействующие на информацию.
2. Причины, виды, каналы утечки и искажение информации.
3. Информационное оружие, его классификация и возможности.
4. Информационное противоборство.
5. Методы нарушения конфиденциальности (целостности, доступности) информации.
6. Национальные интересы РФ и угрозы национальной безопасности.
7. Угрозы информационной безопасности Российской Федерации.
8. Анализ угроз информационной безопасности компьютерных систем.
9. Внешние (внутренние) источники угроз информационной безопасности государства.
10. Актуальные проблемы безопасности компьютерных систем.
11. Актуальные проблемы информационной безопасности при использовании мобильных средств связи.
12. Актуальные проблемы информационной безопасности в социальных сетях.
13. Актуальные проблемы информационной безопасности критически важных объектов.
14. Компьютерная система как объект информационного воздействия.

Критерии оценки в баллах:

5 баллов выставляется студенту, если: 1) студент показал умение выделить основную идею, показать обзор мнений, 2) продемонстрировал свои коммуникативные навыки (не чтение доклада, а рассказ), 3) использованы конкретные примеры из медиапрактики; 4) правильность и своевременность ответов на дополнительные вопросы; 5) грамотно оформил презентацию и оформил доклад в соответствии с требованиями;

4 балла выставляется студенту, если выполнено всего 4 (1-4) из вышеуказанных условий;

3 балла выставляется студенту, если выполнено всего 3 (1-3) из указанных условий;

2 балла выставляется студенту, если он показал общий обзор мнений, не смог ответить на дополнительные вопросы, но оформил доклад в соответствии с требованиями;

1 балл выставляется студенту, если он продемонстрировал неудовлетворительное владение материалом.

Задания для практического задания

Описание практического задания:

1. Описать систему безопасности личного телефона и его приложений.

2. Описать систему безопасности, принятую в любой конкретной редакции.
3. Описать случай утечки важной информации в сфере журналистики.
4. Разработать систему информационной безопасности редакции печатного СМИ.
5. Разработать систему информационной безопасности редакции сетевого СМИ.

Критерии оценки в баллах:

5 баллов выставляется студенту, если:

- 1) студент показал умение выделить основную идею, показать обзор мнений,
- 2) продемонстрировал свои коммуникативные навыки (не чтение доклада, а рассказ),
- 3) использованы конкретные примеры из медиапрактики;
- 4) правильность и своевременность ответов на дополнительные вопросы;
- 5) грамотно оформил презентацию и оформил доклад в соответствии с требованиями;

4 балла выставляется студенту, если выполнено всего 4 (1-4) из вышеуказанных условий;

3 балла выставляется студенту, если выполнено всего 3 (1-3) из указанных условий; **2 балла** выставляется студенту, если он показал общий обзор мнений, не смог ответить на дополнительные вопросы, но оформил доклад в соответствии с требованиями;

1 балл выставляется студенту, если он демонстрировал неудовлетворительное владение материалом.

Примерные вопросы для зачета:

1. Понятие национальной безопасности Российской Федерации.
2. Национальные интересы РФ и стратегические национальные приоритеты.
3. Роль информационной безопасности в обеспечении национальной безопасности государства.
4. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
5. Понятие информационной безопасности Российской Федерации.
6. Интересы личности общества и государства в информационной сфере.
7. Виды угроз информационной безопасности Российской Федерации.
8. Внешние и внутренние источники угроз информационной безопасности Российской Федерации.
9. Методы обеспечения информационной безопасности Российской Федерации
10. Источники понятий в области информационной безопасности.
11. Основные понятия информационной безопасности.
12. Общеметодологические принципы теории информационной безопасности.
13. Понятие и сущность защищаемой информации.
14. Права и обязанности обладателя информации.
15. Виды защищаемой информации.
16. Перечень сведений конфиденциального характера.
17. Понятие интеллектуальной собственности и особенности ее защиты.
18. Понятие угрозы информационной безопасности.
19. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов.
20. Классификация и виды угроз информационной безопасности.
21. Внутренние и внешние источники угроз информационной безопасности.
22. Угрозы утечки информации и угрозы несанкционированного доступа.

23. Основные элементы канала реализации угрозы безопасности информации.
24. Субъекты и цели информационного противоборства.
25. Составные части и методы информационного противоборства.
26. Информационное оружие, его классификация и возможности.
27. Методы нарушения конфиденциальности, целостности и доступности информации.
28. Информационная война как способ воздействия на информационные системы.
29. Информационная безопасность критически важных объектов.
30. Обеспечение безопасности объектов информационной сферы государства в информационной войне.
31. Компьютерная система как объект информационной безопасности.
32. Основные способы защиты информации.
33. Понятие и классификация средств защиты информации.
34. Характеристика средств защиты информации.
35. Уровни информационной безопасности и их характеристика.
36. Сервисы безопасности программно-технического уровня.
37. Идентификация и аутентификация как сервисы безопасности.
38. Управление доступом и его виды.
39. Авторизация как сервис безопасности.
40. Протоколирование и аудит как сервисы безопасности.
41. Криптографические сервисы безопасности.
42. Экранирование как сервис безопасности.
43. Анализ защищенности как сервис безопасности.
44. Туннелирование как сервис безопасности.
45. Управление как сервис безопасности.
46. Назначение формальных моделей безопасности. Политика безопасности.
47. Дискреционная модель безопасности. Модель Харрисона-Руззо-Ульмана.
48. Мандатная модель безопасности. Модель Белла-ЛаПадулы.
49. Формальные модели целостности.
50. Понятие ролевого управления доступом.

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 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов).

Зачтено выставляется студенту, если вопрос раскрыт полностью и без ошибок, отлично знает теоретический материал, ответы аргументированы фактическим материалом

Не зачтено выставляется студенту, если вопрос зачета не раскрыт, студент не знает пройденный материал.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература:

1. Технические средства и методы защиты информации. Учебник для вузов - 7 изд., Шелупанов А.А., Мещеряков Р.В., Зайцев А.П., 2012
2. Криптографические методы защиты информации в телекоммуникационных системах: Учебное пособие, Ветров Ю.В., Макаров С.Б., 2011
3. Сычев Ю.Н. Основы информационной безопасности [Электронный ресурс]: учебное пособие/ Сычев Ю.Н.— Электрон. текстовые данные.— М.: Евразийский открытый институт, 2010.— 328 с.— Режим доступа: <http://www.iprbookshop.ru/10746>.— ЭБС «IPRbooks», по паролю
4. Защита информации техническими средствами: Учебное пособие, Каторин Ю.Ф., Разумовский А.В., Спивак А.И., 2012

Дополнительная литература: 1. Криптография. Вводные главы: Учебное пособие, Пилиди В.С., 2009

2. Информационная безопасность: Учебное пособие, Макаренко С.И., 2009
3. Программно-аппаратные средства обеспечения информационной безопасности: Учебное пособие (2-е издание) Зайцев А.П., Голубятников И.В., Мещеряков Р.В., Шелупанов А.А., 2006

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

1. Windows 8 Russian. Windows Professional 8 Russian Upgrade. Договор №104 от 17.06.2013 г. Лицензия бессрочная.
2. Microsoft Office Standard 2013 Russian. Договор №114 от 12.11.2014 г. Лицензия бессрочная.
3. Офисный пакет LibreOffice. Стандартная общественная лицензия GNU GPL. <https://www.gnu.org/licenses/gpl-2.0.txt>
4. Программа для обработки аудиофайлов – Audacity. Стандартная общественная лицензия GNU GPL <https://www.gnu.org/licenses/gpl-2.0.txt>
5. Программа для обработки графики – GIMP. Стандартная общественная лицензия GNU GPL. <https://www.gnu.org/licenses/gpl-2.0.txt>
6. Настольная издательская система – Scribus. Стандартная общественная лицензия GNU GPL. <https://www.gnu.org/licenses/gpl-2.0.txt>
7. Программа для обработки видеофайлов – OpenShot. Стандартная общественная лицензия GNU GPL. <https://www.gnu.org/licenses/gpl-2.0.txt>

	<i>Учебные и научные ресурсы</i>	<i>Характеристика</i>	<i>Доступ</i>	<i>Регистрация</i>	<i>Ссылка на ресурс</i>
Учебные ресурсы					
1.	Электронно-библиотечная система «Электронный читальный зал»	Полнотекстовая БД учебных и научных электронных изданий, которая включает издания преподавателей	Авторизованный доступ по паролю из любой точки сети Интернет	Регистрация из сети БашГУ, дальнейший доступ из любой точки сети Интернет	https://bashedu.bibliotech.ru/Account/LogOn

		БашГУ			
2.	Электроннобиблиотечная система «Университетская библиотека online»	Полнотекстовая БД учебных и научных электронных изданий	Авторизованный доступ по паролю из любой точки сети Интернет	Регистрация из сети БашГУ, дальнейший доступ из любой точки сети Интернет	http://www.biblioclub.ru/
.	Электроннобиблиотечная система издательства «Лань»	Полнотекстовая БД учебных и научных электронных изданий	Авторизованный доступ по паролю из любой точки сети Интернет	Регистрация из сети БашГУ, дальнейший доступ из любой точки сети Интернет	http://e.lanbook.com/

Российские научные ресурсы

4.	Научная электронная библиотека (eLibrary)	Полнотекстовая и аннотированная БД электронных научных изданий и публикаций в периодических изданиях; доступ к информационноаналитической системе ScienceIndex	Авторизованный доступ по паролю в сети вуза. Пользование ресурсами открытого доступа с любого компьютера в сети Интернет	Регистрация из сети БашГУ	http://elibrary.ru/
5.	База данных «Вестники Московского университета» (на платформе East View)	Полнотекстовая БД научных статей, опубликованных в журнале «Вестник МГУ» (25 серий)	Доступ в сети вуза	Без регистрации	http://online.ebiblioteka.ru/

6.	База данных «Издания по общественным и гуманитарным наукам» (на платформе East View)	Полнотекстовая БД статей, опубликованных в научных журналах (более 80 названий)	Доступ в сети вуза	Без регистрации	http://online.ebiblioteka.ru/
7.	База данных «POLPRED»		Доступ в сети вуза	Без регистрации	http://www.polpred.com/
8.	Электронная база данных диссертаций РГБ	Полнотекстовая БД электронных диссертаций, хранящихся в РГБ	Авторизованный доступ по паролю в сети вуза	Регистрация в Отделе Электронной информации Библиотеки (корпус физмата, к.201)	http://www.diss.rsl.ru/
Зарубежные научные ресурсы					
.	SCOPUS	Наукометрическая, библиографическая и реферативная база данных издательской корпорации Elsevier. Язык английский	Доступ в сети вуза	Без регистрации	http://www.scopus.com/
0.	TaylorandFrancis	Полнотекстовые научные журналы, книги и реферативные журналы. В ресурс включены издания по химии, физике, биологии, наукам о земле, медицине, инженерным и компьютерным наукам, математике, статистике и информатике, а также по экономике и менеджменту, социологии, образованию, праву, филологии, искусствоведению, психологии и т. д. Язык английский	Доступ в сети вуза	Без регистрации	http://www.tandfonline.com/

6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

<i>Наименование специализированных аудиторий, кабинетов, лабораторий</i>	<i>Вид занятий</i>	<i>Наименование оборудования, программного обеспечения</i>
<i>1</i>	<i>2</i>	<i>3</i>
<p>1. Учебная аудитория для проведения занятий лекционного типа: аудитория № 414 (главный корпус), аудитория № 425 (главный корпус).</p> <p>2. Учебная аудитория для проведения занятий семинарского типа: Лаборатория компьютерной филологии № 412 (главный корпус), аудитория № 415, (главный корпус)</p> <p>3. Учебная аудитория для текущего контроля и промежуточной аттестации: Лаборатория ИТ № 312 (главный корпус)</p> <p>4. Помещения для самостоятельной работы: Читальный зал № 1 (главный корпус)</p>	<p>Лекции</p> <p>Практические занятия</p> <p>Промежуточная аттестация</p> <p>Самостоятельная работа</p>	<p>Лаборатория компьютерной филологии №412 Учебная мебель, шкаф, доска, видеочамера Sony PXW-70 – 1 шт., системный блок USN QuadCore 3,2 GHzGb / Hdd 500 Gb / H 81 / TX 450 W / мышь USB / LSD монитор 1,5" / Vin 10 Pro – 2 шт., персональный компьютер i7/H170/8Gb/HDD1Tb/SSD1120/DVD RW/ATX450W/2 – 1 шт.</p> <p>Аудитория № 414. Учебная мебель, учебно-наглядные пособия, экран настенный для проектора DINON Electric L 274*366 MW - 1 шт., проектор мультимедийный MITSUBISHI EX 320U XGA, акустическая система APart MASK 4T-W- 6 шт.</p> <p>Аудитория № 425 Учебная мебель, доска, кафедра, мобильный переносной проектор PJD5226 – 1 шт., экран на штативе 224*183 – 1 шт.</p> <p>Аудитория № 415. Учебная мебель, учебно-наглядные пособия, доска, экран настенный ClassicSolution - 1 шт. модель W 243x182/3 MW-SO/W; проектор мультимедийный EPSON EB-2250U - 1 шт.</p> <p>Лаборатория ИТ № 312 Учебная мебель, доска, учебно-наглядные пособия, трибуна, интерактивная доска SMART с проектором V25 – 1 шт., 12 компьютеров – системный блок USN QuadCore 3,2 GHzGb / Hdd 500 Gb / H 81 / TX 450 W / мышь USB / LSD монитор 1,5" / Vin 10 Pro</p> <p>Читальный зал № 1 Учебная мебель, учебно-наглядные пособия, стенд по пожарной безопасности, моноблоки стационарные – 5 шт., принтер – 1 шт., сканер – 1 шт.</p>

МИНОБРНАУКИ РОССИИ
 ФГБОУ ВО «БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»
 ФАКУЛЬТЕТ БАШКИРСКОЙ ФИЛОЛОГИИ, ВОСТОКОВЕДЕНИЯ И
 ЖУРНАЛИСТИКИ

СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины «Информационная безопасность» на 8 семестр

очная

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 / 108
Учебных часов на контактную работу с преподавателем:	36,2
лекций	18
практических/ семинарских	18
лабораторных	
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	0,2
Учебных часов на самостоятельную работу обучающихся (СР)	71,8
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	

Форма(ы) контроля:
зачет 8 семестр

№ п/п	Тема и содержание	Форма изучения материалов: лекции, практические занятия, семинарские занятия, лабораторные работы, самостоятельная работа и трудоемкость (в часах)				Основная и дополнительная литература, рекомендуемая студентам (номера из списка)	Задания по самостоятельной работе студентов	Форма текущего контроля успеваемости (коллоквиумы, контрольные работы, компьютерные тесты и т.п.)
		ЛК	ПР/СЕМ	ЛР	СР			
1	2	3	4	5	6	7	8	9
	<p>Введение в информационную безопасность.</p> <p>Роль и место системы обеспечения информационной безопасности (ИБ) в системе национальной безопасности РФ; доктрина ИБ, история проблемы ИБ, угрозы ИБ; методы и средства обеспечения ИБ; методологические и технологические основы комплексного обеспечения ИБ; модели, стратегии и системы обеспечения ИБ; методы управления, организации и обеспечения работ по обеспечению ИБ;</p>	4	3		2	О – 1-4; Д – 1-3	Самостоятельное изучение литературы (подготовить доклад)	опрос, проверка доклада

	проблемы информационной войны; правовые и нормативные акты в области ИБ.							
2.	Защита от компьютерных вирусов История появления компьютерных вирусов и факторы, влияющие на их распространение. Понятие компьютерного вируса. Основные этапы жизненного цикла вирусов. Объекты внедрения, режимы функционирования и специальные функции вирусов. Схемы заражения файлов. Схемы заражения загрузчиков. Способы маскировки, используемые вирусами. Классификация компьютерных вирусов. Общая организация защиты от компьютерных вирусов	6	7		4	О – 1-4; Д – 1-3	Самостоятельное изучение литературы (подготовить доклад)	опрос, проверка доклада

3.	<p>Защита от потери информации и отказов программно-аппаратных средств. Уничтожение остаточных данных. Виды остаточных данных. Способы защиты от несанкционированного использования остаточной информации. Использование специализированных программ по уничтожению остаточных данных. Специальные режимы и особенности шифрования данных в режиме реального времени с возможность мгновенного уничтожения данных. Использование общесистемных и специализированных программных средств для мгновенного уничтожения данных. Основные способы защиты от потери информации и нарушений работоспособности вычислительных средств. Внесение функциональной и информационной избыточности. Способы резервирования информации. Правила обновления резервных данных. Методы сжатия информации. Архивация файловых данных</p>	8	8		4	1-3 О – 1-4; Д –	Самостоятельное изучение литературы (подготовить доклад)	опрос, проверка доклада
Всего часов: 108		18	18		71,8			