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

Утверждено:
на заседании кафедры
протокол № 7 от «18» февраля 2022 г.

Зав. кафедрой _____/ Исмагилова А.С.

Согласовано:
Председатель УМК института

_____/ Гильмутдинова Р.А.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

Б1.О.23 Цифровая гигиена

Обязательная часть

программа специалитета

Специальность
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Специализация
Организация и технологии защиты информации (по отраслям)

Квалификация
Специалист по защите информации

Разработчик (составитель)
профессор, д-р физ.-мат. наук, доцент
(должность, ученая степень, ученое звание)

_____ /Исмагилова А.С.
(подпись, Фамилия И.О.)

Для приема: 2022 г.

Уфа 2022 г.

Составитель: Исмагилова Альбина Сабирьяновна, д.ф.-м.н., профессор кафедры управления информационной безопасностью

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

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

Дополнения и изменения, внесенные в рабочую программу дисциплины, утверждены на заседании кафедры ____,
протокол № ____ от «____» ____________ 20 _ г.

Заведующий кафедрой ___________________/ _____________Ф.И.О/

СОДЕРЖАНИЕ

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
Командная работа и лидерство	УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.	УК-3.1. Знает общие формы организации деятельности коллектива; основы стратегического планирования работы коллектива для достижения поставленной цели.	Знать научно-техническую литературу, нормативные и методические материалы по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.
		УК-3.2. Умеет учитывать в своей социальной и профессиональной деятельности интересы коллег; предвидеть результаты (последствия) как личных, так и коллективных действий; планировать командную работу.	Уметь организовывать и поддерживать выполнение комплекса мер по информационной безопасности.
		УК-3.3. Владеет навыками постановки цели в условиях командой работы; способами управления командной работой в решении поставленных задач.	Владеть методами управления информационной безопасности автоматизированных систем.

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Основы цифровой гигиены» относится к группе дисциплин основной части образовательной программы.

Дисциплина изучается на 3 курсе в 5 и 6 семестрах.

Целью изучения дисциплины является раскрытие содержания основных понятий и формальных моделей обеспечения безопасности компьютерных систем и призвана сформировать у обучающихся теоретико-методологические основы профессиональной деятельности в сфере компьютерной 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

УК-3. Способен организовывать и руководить работой команды, вырабатывая командную стратегию для достижения поставленной цели.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения	
		«Не зачтено»	«Зачтено»
УК-3.1. Знает общие формы организации деятельности коллектива; основы стратегического планирования работы коллектива для достижения поставленной цели.	Знать научно-техническую литературу, нормативные и методические материалы по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.	Не знает научно-техническую литературу, нормативные и методические материалы по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.	Знает научно-техническую литературу, нормативные и методические материалы по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.
УК-3.2. Умеет учитывать в своей социальной и профессиональной деятельности интересы коллег; предвидеть результаты (последствия) как личных, так и коллективных действий; планировать командную работу.	Уметь организовывать и поддерживать выполнение комплекса мер по информационной безопасности.	Не умеет организовывать и поддерживать выполнение комплекса мер по информационной безопасности.	Умеет организовывать и поддерживать выполнение комплекса мер по информационной безопасности.
УК-3.3. Владеет навыками постановки цели в	Владеть методами управления информационной	Не владеет методами управления информационной	Владеет методами управления информационной

условиях командой работы; способами управления командной работой в решении поставленных задач.	безопасности автоматизированных систем.	безопасности автоматизированных систем.	безопасности автоматизированных систем.

Критериями оценивания являются баллы, которые выставляются преподавателем за виды деятельности (оценочные средства) по итогам изучения модулей (разделов дисциплины), перечисленных в рейтинг-плане дисциплины (для зачета: текущий контроль – максимум 50 баллов; рубежный контроль – максимум 50 баллов, поощрительные баллы – максимум 10).

Шкалы оценивания:

зачтено – от 60 до 110 рейтинговых баллов (включая 10 поощрительных баллов),

не зачтено – от 0 до 59 рейтинговых баллов).

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
УК-3.1. Знает общие формы организации деятельности коллектива; основы стратегического планирования работы коллектива для достижения поставленной цели.	Знать научно-техническую литературу, нормативные и методические материалы по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.	Не знает научно-техническую литературу, нормативные и методические материалы по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.	Знает некоторые нормативные и методические материалы по вопросам обеспечения информационной.	Знает научно-техническую литературу, некоторые нормативные и методические материалы по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.	Знает научно-техническую литературу, нормативные и методические материалы по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.
УК-3.2. Умеет учитывать в своей социальной и профессионал	Уметь организовывать и поддерживать выполнение комплекса мер по	Не умеет организовывать и поддерживать выполнени	Умеет в некоторых ситуациях поддерживать выполнение	Умеет поддерживать выполнение комплекса мер по	Умеет организовывать и поддерживать выполнение

ьной деятельности интересы коллег; предвидеть результаты (последствия) как личных, так и коллективных действий; планировать командную работу.	информационной безопасности.	е комплекса мер по информационной безопасности.	мер по обеспечению информационной безопасности.	информационной безопасности.	комплекса мер по информационной безопасности.
УК-3.3. Владеет навыками постановки цели в условиях командой работы; способами управления командной работой в решении поставленных задач.	Владеть методами управления информационной безопасности автоматизированных систем.	Не владеет методами управления информационной безопасности автоматизированных систем.	Владеет некоторыми методами управления информационной безопасности.	Владеть некоторыми методами управления информационной безопасности автоматизированных систем.	Владеет методами управления информационной безопасности автоматизированных систем.

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).

Шкалы оценивания:

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
УК-3.1. Знает общие формы	Знать научно-техническую литературу, нормативные и	Т, ПР, ЛР

организации деятельности коллектива; основы стратегического планирования работы коллектива для достижения поставленной цели.	методические материалы по вопросам обеспечения информационной безопасности по профилю своей профессиональной деятельности.	
УК-3.2. Умеет учитывать в своей социальной и профессиональной деятельности интересы коллег; предвидеть результаты (последствия) как личных, так и коллективных действий; планировать командную работу.	Уметь организовывать и поддерживать выполнение комплекса мер по информационной безопасности.	
УК-3.3. Владеет навыками постановки цели в условиях командой работы; способами управления командной работой в решении поставленных задач.	Владеть методами управления информационной безопасности автоматизированных систем.	

Т - тестирование, ПР - практические работы

Рейтинг-план дисциплины
5 семестр

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1				
Текущий контроль				5
Аудиторная работа (практические работы)	5	1	0	5
Рубежный контроль				17
Тест 1	0,5	34	0	17
Всего				**22**
Модуль 2				
Текущий контроль				17
Аудиторная работа (практические работы)	3; 6; 8	3	0	17
Рубежный контроль				17
Тест 2	0,5	34	0	17
Всего				**34**
Модуль 3				
Текущий контроль				28
Аудиторная работа (практические, лабораторные работы)	3; 3; 3; 4; 4; 5; 6	6	0	28
Рубежный контроль				16
Тест 3	0,5	32	0	16
Всего				**44**
Поощрительные баллы				
1. Студенческая олимпиада			0	4
2. Публикация статей, участие в конференции			0	6
Всего				**10**
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Зачет				

6 семестр

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
Модуль 1				
Текущий контроль			0	20
Аудиторная работа (практические, лабораторные работы)	10	2	0	20
Рубежный контроль				15
Тест	15	1		15
Всего				**35**
Модуль 2				
Текущий контроль				20
Аудиторная работа (практические, лабораторные работы)	10	2	0	20
Рубежный контроль				15
Тест	15	1	0	15
Всего				**35**
Поощрительные баллы				
1. Студенческая олимпиада			0	4
2. Публикация статей, участие в конференции			0	6
Всего				**10**
Посещаемость (баллы вычитаются из общей суммы набранных баллов)				
3. Посещение лекционных занятий				-6
4. Посещение практических занятий				-10
Итоговый контроль				
Экзамен			0	30

Тестирование

Модуль 1.

1. Для чего служит фильтрация контента?
а) Защищает от скрытой загрузки вредоносного программного обеспечения
б) Помогает быстро находить в сети требуемый контент сохраняя при этом много драгоценного времени
в) Отключает назойливую рекламу
г) Отсеивает поисковый спам

2. Какой уровень безопасности трафика обеспечивает WPA2?
а) Высокий
б) Низкий
в) Достаточный для домашней сети
г) Средний

Модуль 2.

1. Что такое Brute Force?
а) Взлом методом заражения системы через вредоносный файл
б) Метод заставляющий пользователя самому раскрыть конфиденциальную информацию
в) Получение конфиденциальной информации с компьютера методом электронной рассылки
г) Взлом методом перебора паролей

2. Как называется преднамеренно внесенный в программное обеспечение объект, приводящий к действиям программного обеспечения не предусмотренным производителем, приводящим к нарушению конфиденциальности и целостности информации?
а) Троян
б) Бэкдор
в) Закладка
г) Вирус

Темы практических работ

Модуль 1.

1. Содержание и основные понятия компьютерной безопасности.
2. Угрозы безопасности в компьютерных системах.
3. Политика и модели безопасности в компьютерных системах.
4. Модели безопасности на основе дискреционной политики.
5. Модели безопасности на основе мандатной политики.
6. Модели безопасности на основе тематической политики.
7. Модели безопасности на основе ролевой политики.

Модуль 2.

1. Автоматные и теоретико-вероятностные модели информационного невлияния и информационной невыводимости.
2. Модели и механизмы обеспечения целостности данных.
Методы и технологии обеспечения доступности (сохранности) данных.
3. Политика и модели безопасности в распределенных компьютерных системах.
4. Методы, критерии и шкалы оценки защищенности (безопасности) компьютерных систем.
5. Теоретико-графовые модели комплексной оценки защищенности компьютерных систем.
6. Методы анализа и оптимизации индивидуально-групповых систем разграничения доступа.

Перечень вопросов для экзамена

1. Составляющие модели безопасности - модель (формализация) компьютерной системы в аспекте безопасности информации, критерии, формализованные правила, алгоритмы, механизмы безопасного функционирования КС.
2. Класс моделей конечных состояний. Компьютерная система как автомат (процесс) с дискретным временем функционирования.
3. Теоретико-множественная субъектно-объектная формализация (модель) компьютерной системы.
4. Понятие субъекта и объекта, потока информации и доступа субъекта к объекту, методов и прав доступа, разграничения доступа.
5. Основные типы политик безопасности — дискреционная, мандатная, тематическая, ролевая, временная, маршрутная.
6. Программно-техническая структура компьютерной системы в контексте безопасности.
7. Гарантирование выполнения политики безопасности. Тождественность объектов и тождественность субъектов доступа (неизменность свойств).
8. Общая характеристика политики дискреционного доступа. Тройки доступа: субъект-операция-объект.
9. Модели дискреционного (избирательного) разграничения доступа и модели распространения прав доступа.
10. Пятимерное пространство Хартсона как пример выражения дискреционного разграничения доступа на языке реляционной алгебры.
11. Модели разграничения доступа на основе матрицы доступа.
12. Модель распространения прав доступа Харисона-Руззо-Ульмана.
13. Модель типизованной матрицы доступа как расширение модели Харисона-Руззо-Ульмана и способ разрешения проблемы троянских программ.
14. Теоретико-графовая модель TAKE-GRANT для исследования распространения прав доступа в системах с добровольным управлением доступом.
15. Расширенная (extended) модель TAKE-GRANT. Неявные (вероятностные) каналы утечки информации и «мнимые» дуги в графе доступов.
16. Общая характеристика политики мандатного (полномочного) доступа.
17. Модель безопасности Белла-ЛаПадулы. Критерий безопасного состояния системы. Функция перехода системы из одного состояния в другое.
18. Расширения модели Белла-ЛаПадулы. Безопасная функция перехода МакЛина и теорема безопасности МакЛина, разрешение проблемы Z-системы.
19. Общая характеристика политики тематического доступа. Тематическое классификационное множество и ее разновидности. Способы тематической классификации субъектов и объектов доступа на основе дескрипторных, иерархических и фасетных классификационных множеств.
20. Тематические решетки на основе классификационных множеств. Решетка подмножеств множества тематических рубрик при дескрипторной классификации.
21. Модель тематико-иерархического разграничения доступа в системах с мультирубрицированной тематической классификацией субъектов и объектов доступа.
22. Общая характеристика политики ролевого (типизованного) доступа.
23. Разновидности ролевых систем по отношениям ролей, принципам назначения ролей пользователям и сеансовой авторизации пользователей с назначенными ролями.
24. Системы с иерархической организацией ролей, с взаимоисключающими в системе ролями (статическое распределение обязанностей), с взаимоисключающими в рамках одного сеанса ролями (динамическое распределение обязанностей) и др.
25. Модель индивидуально-группового доступа.
26. MMS-модель (military message system) Лендвера-МакЛина как пример сочетания дискреционной, мандатной и ролевой политики безопасности.

27. Автоматная модель информационного невлияния Гогена-Мессигера.
28. Теоретико-вероятностная трактовка информационного потока (по К.Шеннону). Модели информационной невыводимости и информационного невлияния как теоретико-методологическая основа анализа (выявления) и перекрытия скрытых каналов «по памяти» и «по статистике».
29. Дискреционная модель обеспечения целостности данных Кларка-Вильсона.
30. Мандатная модель К.Биба. Уровни целостности данных. Уровни доверия пользователям. Правила мандатного доступа, не нарушающие целостность данных.
31. Проблемы и разновидности совместимости в практической реализации моделей Белла-ЛаПадулы и К.Биба: на основе двух разных решеток безопасности, на основе одной общей решетки, но с двумя отдельными метками для объектов и субъектов.
32. Транзакционная парадигма коллективной (одновременной) обработки данных в клиент-серверных системах.
33. Протоколы выполнения и фиксации транзакций. Протоколы, основанные на «захватах» блокировках объектов. Двухфазной протокол выполнения и фиксации транзакций.
34. Резервирование, архивирование и журнализация данных.
35. Понятие «распределенности» компьютерных систем в аспекте безопасности. Дополнительные аспекты политики безопасности в распределенных компьютерных системах.
36. Модель безопасности Варахаратжана. Фазы доступа.
37. Зональная политика безопасности и ее теоретико-множественное формализация (модель).
38. Понятие измерения величин и оценки объектов как отображения множеств с отношениями. Процесс измерения (оценки) и шкала измерения (оценки). Точные измерения и измерения с погрешностями.
39. Оценка защищенности (безопасности) компьютерных систем как задача многомерного шкалирования свойств КС в аспекте безопасности.
40. Теоретико-графовая модель систем защиты с полным перекрытием [угроз] на основе двудольного графа «Угрозы-Объекты». Модель Клементса.
41. Разновидности теоретико-графового подхода к моделированию систем комплексной оценки защищенности в виде трехдольных графов.
42. Тактико-техническое обоснование систем защиты.
43. Теоретико-графовая формализация (модель) систем индивидуально-группового назначения пользователям (субъектам доступа) прав доступа к иерархически организованным ресурсам (объектам доступа).
44. Матричные соотношения для вычисления итоговых прав доступа. Коэффициенты дублирования прав доступа, превышения и недостатка прав доступа как количественные параметры оптимизации систем индивидуально-группового доступа и их матричные выражения.
45. Методы проектирования системы рабочих групп пользователей - «сверху» и «снизу». Выражение для вычисления меры близости пользователей по требуемым правам доступа.

Образец экзаменационного билета

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Башкирский государственный университет»
Институт истории и государственного управления

Направление
10.05.05 Безопасность информационных технологий в правоохранительной сфере

Дисциплина
«Цифровая гигиена»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 5

1. Класс моделей конечных состояний. Компьютерная система как автомат (процесс) с дискретным временем функционирования.
2. Модель безопасности Варахаратжана. Фазы доступа.

Зав. кафедрой управления информационной безопасностью /А.С. Исмагилова /

Примерные критерии оценивания ответа на экзамене (только для тех, кто учится с использованием модульно-рейтинговой системы обучения и оценки успеваемости студентов):

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.

5. Учебно-методическое и информационное обеспечение дисциплины

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

Основная литература:

1. Садердинов А. А. Информационная безопасность предприятия : учеб. пособие / Садердинов, Али Абдулович ; В.А.Трайнёв, А.А.Федулов; Междунар. акад. наук информации, информ. процессов и технологий. - 3-е изд. - М. : Дашков и К, 2006. - 335 с. - ISBN 5-94798-918-2 : 154-00.

2. Шаньгин В. А. Информационная безопасность компьютерных систем и сетей : учеб. пособие для студентов учреждений сред. проф. образования, обуч. по группе специальностей 2200 "Информатика и вычислительная техника" / Шаньгин, Владимир Фёдорович. - М. : ФОРУМ: ИНФРА-М, 2008. - 415 с. - (Профессиональное образование). - Рекомендовано МО РФ. - 194-92.

3. Галатенко В. А. Основы информационной безопасности : учеб. пособие для студентов вузов, обуч. по специальности 351400 "Прикл. информ." / Галатенко, Владимир Антонович. - 4-е изд. - М. : Изд-во Интернет-Ун-та Информ. Технологий: БИНОМ. Лаб. знаний, 2016, 2008, 2006. - 205 с. - (Основы информационных технологий). - Рекомендовано УМО. - ISBN 978-5-94774-821-5 : 230-00.

4. Герман О. Н. Теоретико-числовые методы в криптографии : учеб. для студентов учреждений высш. проф. образования / Герман, Олег Николаевич, Ю. В. Нестеренко. - М. : Академия, 2012. - 270,[1] с. - (Высшее профессиональное образование. Информатика и вычислительная техника). - ISBN 978-5-7695-6786-5 : 603-90.

5. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства :

учебное пособие / В. Ф. Шаньгин ; Шаньгин В. Ф. - М. : ДМК Пресс, 2010. - 544. - ISBN 978-5-94074-518-1.

Дополнительная литература:

6. Казанцева С.Я.. Правовое обеспечение информационной безопасности : [учеб. пособие для вузов по специальностям 075200 "Компьютер. безопасность", 075500 "Комплекс. обеспечение информ. безопасности и автоматизир. систем", 075600 "Информ. безопасность телекоммуникац. систем" / С.Я.Казанцев и др.]; под ред. С.Я.Казанцева. - М. : Academia, 2005. - 239 с. : ил. ; 22 см. - (Высшее профессиональное образование. Информационная безопасность). - Библиогр.: с. 235-237. - Допущено УМО. - ISBN 5-7695-1209-1 : 129-47.

7. Панасенко, Сергей Петрович. Основы криптографии для экономистов : учеб. пособие / Панасенко, Сергей Петрович ; В.П.Батура; под ред. Л.Г.Гагариной. - М. : Финансы и статистика, 2005. - 173,[1] с. - ISBN 5-279-02938-6 : 120-00.

8. Душин, Владимир Константинович. Теоретические основы информационных процессов и систем : учебник / Душин, Владимир Константинович. - 2-е изд. - М. : Дашков и К, 2006. - 347,[1] с. : ил. - Рекомендовано МО РФ. - ISBN 5-94798-869-0 : 121-33.

9. Филин, Сергей Александрович. Информационная безопасность : учеб. пособие / Филин, Сергей Александрович. - М. : Альфа-Пресс, 2006. - 411 с. - ISBN 5-94280-163-0 : 129-03.

10. Расторгуев, Сергей Павлович. Основы информационной безопасности : учеб. пособие для студентов вузов, обуч. по специальности "Компьютер. безопасность", "Комплекс. обеспечение информ. безопасности автоматизир. систем" и "Информ. безопасность телеком. систем" / Расторгуев, Сергей Павлович. - М. : Академия, 2007. - 186,[1] с. - (Высшее профессиональное образование. Информационная безопасность). - Допущено УМО. - ISBN 978-5-7695-3098-2 : 150-70.

11. Белов Е. Б. Основы информационной безопасности : [учеб. пособие для вузов] / Е. Б. Белов. - М. : Горячая линия - Телеком, 2006. - 544 с. - ISBN 5-93517-292-5 : 154-00.

12. Корнеев, Игорь Константинович. Защита информации в офисе : учебник / Корнеев, Игорь Константинович, Е. А. Степанов. - М. : Проспект, 2010. - 150-00.
13. Петров С. В. Информационная безопасность : учеб. пособие / С. В. Петров. - Новосибирск: АРТА, 2012. - 439-77.

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

1. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
2. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
3. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
4. www.fstec.ru –сайт ФСТЭК России
5. www.fsb.ru – сайт ФСБ России
6. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
7. 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);
8. www.newlibrary.ru – Новая электронная библиотека;
9. www. edu.ru – Федеральный портал российского образования;
10. www.elibrary.ru – Научная электронная библиотека;
11. www.nehudlit.ru – Электронная библиотека учебных материалов.
12. 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.
13. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
14. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

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

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения	
1. *учебная аудитория для проведения занятий лекционного типа:* аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416	Лекции, практические занятия, лабораторные занятия, курсовое проектирование (выполнение курсовых работ), групповые и	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387	1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic

(гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). **2.** ***учебная аудитория для проведения лабораторных работ:*** компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус), Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности аудитория №507 (гуманитарный корпус). **3.** ***учебная аудитория для проведения занятий семинарского типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус). **4.** ***учебная аудитория для курсового проектирования (выполнения курсовых работ):***аудитория №613 (гуманитарный корпус). **5.** ***учебная аудитория для проведения***	индивидуальные консультации, текущий контроль, промежуточная аттестация	RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV(XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ MA1225 – 1 шт. **Аудитория № 415** Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ MA1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер	Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

групповых и индивидуальных консультаций: аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **6. *учебная аудитория для текущего контроля и промежуточной аттестации:*** аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус). **7. *помещения для самостоятельной***		встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 610** Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м. **Аудитория № 613** Учебная мебель, доска, моноблок стационарный – 15 шт. **Компьютерный класс аудитория № 420** Учебная мебель, моноблоки стационарные 15 шт. **Компьютерный класс аудитория № 404** Учебная мебель, компьютеры -15 штук. **Аудитория 402 читальный зал библиотеки** Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные. **Лаборатория систем и сетей передачи данных, сетей и систем передачи информации, программно-аппаратных средств обеспечения информационной безопасности № 507** Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технические средства обработки информации, стенд "Устройство ПК". **Аудитория № 523** Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.	

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

Приложение 1

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

Содержание рабочей программы
дисциплины **Основы цифровой гигиены**
на 5 семестр ОФО

Вид работы	**Объем дисциплины**
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часа
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 контроля:
зачет 5 семестр

Содержание рабочей программы
дисциплины **Основы цифровой гигиены**
на 6 семестр ОФО

Вид работы	**Объем дисциплины**
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часа
Учебных часов на контактную работу с преподавателем:	33,2
лекций	16
практических/ семинарских	16
лабораторных	
других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем) (ФКР)	1,2
Учебных часов на самостоятельную работу обучающихся (СР)	47,8
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	27

Форма контроля:
экзамен 6 семестр

№	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	ЛР	СРС			
1	2	3	4	5	6	7	8	9
5 семестр								
1	Содержание и основные понятия компьютерной безопасности.	2	2		10	1 - 4	Самостоятельное изучение рекомендуемых источников и материалов	Т, ПР
2	Угрозы безопасности в компьютерных системах.	4	4		14	1 - 4	Самостоятельное изучение рекомендуемых источников и материалов	Т, ПР
3	Политика и модели безопасности в компьютерных системах.	4	4		16	1 - 4	Самостоятельное изучение рекомендуемых источников и материалов	Т, ПР
4	Модели безопасности на основе дискреционной политики.	4	4		15,2	1 - 4	Самостоятельное изучение рекомендуемых источников и материалов	Т, ПР
5	Модели безопасности на основе мандатной политики.	4	4		16	1 - 4	Самостоятельно	Т, ПР

	Модели безопасности на основе тематической политики. Модели безопасности на основе ролевой политики.						е изучение рекомендуемых источников и материалов	
	Всего	18	18		71,2			
6 семестр								
6	Автоматные и теоретико-вероятностные модели информационного невлияния и информационной невыводимости.	2	2		8	1 - 4	Самостоятельное изучение рекомендуемых источников и материалов	Т, ПР
7	Модели и механизмы обеспечения целостности данных. Методы и технологии обеспечения доступности (сохранности) данных.	2	2		8	1 - 4	Самостоятельное изучение рекомендуемых источников и материалов	Т, ПР
8	Политика и модели безопасности в распределенных компьютерных системах.	2	2		8	1 - 4	Самостоятельное изучение рекомендуемых источников и материалов	Т, ПР
9	Методы, критерии и шкалы оценки защищенности (безопасности) компьютерных систем.	2	2		8	1 - 4	Самостоятельное изучение рекомендуемых источников и материалов	Т, ПР
10	Теоретико-графовые модели комплексной оценки защищенности компьютерных систем.	4	4		8		Самостоятельное изучение рекомендуемых источников и материалов	Т, ПР
11	Методы анализа и оптимизации индивидуально-групповых систем разграничения доступа.	4	4		7,8		Самостоятельное изучение рекомендуемых источников и материалов	Т, ПР

	Всего	16	16		47,8			

Т - тестирование, ПР - практические работы