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)

Б1.В.ДВ.01.01 Основы безопасности критической информационной инфраструктуры

Часть, формируемая участниками образовательных отношений

программа бакалавриата

Направление подготовки
10.03.01 Информационная безопасность

Направленность (профиль) подготовки
Организация и технологии защиты информации (в системе государственного и муниципального управления)

Квалификация
бакалавр

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

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

Для приема: 2021 г.

Уфа 2021 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 № 8 от «24» февраля 2021 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
	ПК-3. Способен организовать мониторинг защищенности информации в автоматизированных системах	ПК-3.1. Знает научно-техническую литературу, нормативные и методические материалы по методам обеспечения информационной безопасности автоматизированных систем.	Знать особенности и способы применения программных и программно-аппаратных средств защиты информации; методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации.
		ПК-3.2. Умеет разрабатывать и реализовывать планы информатизации предприятий и обеспечения их информационной безопасности на основе современных программно-аппаратных систем с учетом особенностей объектов защиты.	Уметь устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств

			защиты информации.
		ПК-3.3. Имеет навыки разработки технических заданий на проектирование, в выполнении технических и рабочих проектов подсистем информационной безопасности предприятия и автоматизированных систем с учетом действующих нормативных и методических документов.	Владеть навыками установки, настройки программных средств защиты информации в автоматизированной системе; навыками обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; навыками тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации.

2. Цель и место дисциплины в структуре образовательной программы

Дисциплина «Основы безопасности критической информационной инфраструктуры» относится к группе дисциплин части, формируемой участниками образовательных отношений образовательной программы.

Дисциплина изучается на 4 курсе в 7 семестре.

Целью изучения дисциплины является освоение обучающимися теоретических аспектов вопроса обеспечения информационной безопасности критических информационных инфраструктур посредством анализа существующих подходов и принципов.

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-8. Способен создавать и поддерживать в повседневной жизни и в профессиональной деятельности безопасные условия жизнедеятельности для сохранения природной среды, обеспечения устойчивого развития общества, в том числе при угрозе и возникновении чрезвычайных ситуаций и военных конфликтов.

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
ПК-3.1. Знает научно-техническую литературу, нормативные и методические материалы по методам обеспечения информационной безопасности автоматизированных систем.	Знать особенности и способы применения программных и программно-аппаратных средств защиты информации; методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации.	Не знает особенности и способы применения программных и программно-аппаратных средств защиты информации; методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; типовые модели управления доступом, средств,	Знает особенности и способы применения программных и программно-аппаратных средств защиты информации.	Знает особенности и способы применения программных и программно-аппаратных средств защиты информации; методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации.	Знает особенности и способы применения программных и программно-аппаратных средств защиты информации; методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации.

		методов и протоколов идентификации и аутентификации.			
ПК-3.2. Умеет разрабатывать и реализовывать планы информатизации предприятий и обеспечения их информационной безопасности на основе современных программно-аппаратных систем с учетом особенностей объектов защиты.	Уметь устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации.	Не умеет устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации.	Уметь настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями.	Умеет устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями.	Умеет устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации.

ПК-3.3. Имеет навыки разработки технических заданий на проектирование, в выполнении технических и рабочих проектов подсистем информационной безопасности предприятия и автоматизированных систем с учетом действующих нормативных и методических документов.	Владеть навыками установки, настройки программных средств защиты информации в автоматизированной системе; навыками обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; навыками тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации.	Не владеет навыками установки, настройки программных средств защиты информации в автоматизированной системе; навыками обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; навыками тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации.	Владеет навыками установки, настройки программных средств защиты информации в автоматизированной системе.	Владеет навыками установки, настройки программных средств защиты информации в автоматизированной системе; навыками обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами.	Владеет навыками установки, настройки программных средств защиты информации в автоматизированной системе; навыками обеспечения защиты автономных автоматизированных систем программными и программно-аппаратными средствами; навыками тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации.

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**
ПК-3.1. Знает научно-техническую литературу, нормативные и методические материалы по методам обеспечения информационной безопасности автоматизированных систем.	Знать особенности и способы применения программных и программно-аппаратных средств защиты информации; методы тестирования функций отдельных программных и программно-аппаратных средств защиты информации; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации.	Т, ПР
ПК-3.2. Умеет разрабатывать и реализовывать планы информатизации предприятий и обеспечения их информационной безопасности на основе современных программно-аппаратных систем с учетом особенностей объектов защиты.	Уметь устанавливать, настраивать, применять программные и программно-аппаратные средства защиты информации; устанавливать и настраивать средства антивирусной защиты в соответствии с предъявляемыми требованиями; диагностировать, устранять отказы, обеспечивать работоспособность и тестировать функции программно-аппаратных средств защиты информации.	
ПК-3.3. Имеет навыки разработки технических заданий на проектирование, в выполнении технических и рабочих проектов подсистем	Владеть навыками установки, настройки программных средств защиты информации в автоматизированной системе; навыками обеспечения защиты автономных автоматизированных систем	

информационной безопасности предприятия и автоматизированных систем с учетом действующих нормативных и методических документов.	программными и программно-аппаратными средствами; навыками тестирования функций, диагностика, устранения отказов и восстановления работоспособности программных и программно-аппаратных средств защиты информации.	

Т - тестирование, ПР - практические работы

Рейтинг-план дисциплины

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)				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
Итоговый контроль				
Экзамен			0	30

Тестирование

Модуль 1.

1. Полномочия ФСТЭК в отношении безопасности КИИ

а) Утверждение формы направления сведений о результатах категоризации объектов КИИ

б) Установление требований по обеспечению безопасности значимых объектов КИИ и к созданию систем безопасности таких объектов

в) Внесение предложений о совершенствовании нормативно-правового регулирования

г) Правовое регулирование деятельности Национального координационного центра по компьютерным инцидентам и координация действий субъектов КИИ

2. Полномочия ФСБ в отношении безопасности КИИ

а) Утверждение формы направления сведений о результатах категоризации объектов КИИ

б) Установление требований по обеспечению безопасности значимых объектов КИИ и к созданию систем безопасности таких объектов

в) Внесение предложений о совершенствовании нормативно-правового регулирования

г) Правовое регулирование деятельности Национального координационного центра по компьютерным инцидентам и координация действий субъектов КИИ

Модуль 2.

1. Обязанности субъектов КИИ в отношении ФЗ № 187

а) Провести категорирование объектов КИИ

б) Обеспечить интеграцию в ГосСОПКА

в) Обеспечить безопасности объектов КИИ посредством внедрения организационных и технических мер

г) Внести предложения о совершенствовании нормативно-правового регулирования

2. К организационным методам обеспечения информационной безопасности критической информационной инфраструктуры относятся:

а) Организация внутри объектового и пропускного режима и охраны

б) Комплексное планирование мероприятий по защите информации

в) Лицензионные соглашения и контракты

г) Меры ответственности за нарушение правил защиты

Темы практических работ

Модуль 1.

1. Правовые основы понятия критической информационной инфраструктуры.
2. Методы обеспечения информационной безопасности критической информационной инфраструктуры.
3. Принципы обеспечения комплексной безопасности критической информационной инфраструктуры.
4. Уязвимости и угрозы безопасности организации.

Модуль 2.

1. Выявление критических процессов и определение объектов критической информационной инфраструктуры организации.
2. Модель актуальных угроз безопасности объектов критической инфраструктуры организации.
3. Категорирование объектов критической информационной инфраструктуры организации.
4. Комплекс мер и методов обеспечения информационной безопасности.
5. Нейтрализация актуальных угроз.

Перечень вопросов для экзамена

1. Правовые основы понятия критической информационной инфраструктуры.
2. Критическая информационная инфраструктура как объект обеспечения безопасности.
3. Анализ существующих методов обеспечения информационной безопасности критической информационной инфраструктуры.
4. Принципы обеспечения комплексной безопасности критической информационной инфраструктуры.
5. Изучение деятельности и организационной структуры организации, осуществляющей медицинскую деятельность.
6. Анализ технической архитектуры организации, осуществляющей медицинскую деятельность.
7. Анализ программной архитектуры и данных, обрабатываемых медицинской организацией.
8. Анализ обрабатываемых в медицинской организации данных.
9. Выявление критических процессов и определение объектов критической информационной инфраструктуры организации, осуществляющей медицинскую деятельность.
10. Оценка факторов активности потенциального злоумышленника в контексте информационной безопасности организации, осуществляющей медицинскую деятельность.
11. Анализ уязвимостей и угроз безопасности организации, осуществляющей медицинскую деятельность.
12. Разработка модели актуальных угроз безопасности объектов критической инфраструктуры организации, осуществляющей медицинскую деятельность.
13. Определение категории выявленных объектов критической информационной инфраструктуры организации, осуществляющей медицинскую деятельность.
14. Определение оптимального комплекса организационных мер и методов обеспечения информационной безопасности.
15. Определение оптимального комплекса программно-аппаратных мер и методов обеспечения информационной безопасности в части технической и физической защиты.
16. Разработка мер защиты информации в целях нейтрализации выявленных актуальных угроз.

Образец экзаменационного билета

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

Направление
10.03.01Информационнаябезопасность

Дисциплина
«Основы безопасности критической информационной инфраструктуры»

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 5

1. Правовые основы понятия критической информационной инфраструктуры.
2. Анализ уязвимостей и угроз безопасности организации, осуществляющей медицинскую деятельность.

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

Федерации (от 17.02.2018 г. № 162) [Электронный ресурс], информационно-правовой портал: http://www.garant.ru/products/ipo/prime/doc/71783452/

6. Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования: Приказ ФСТЭК (от 21.12.2017 №235) [Электронный ресурс] : сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/index?id=1606:prikaz-fstek-rossii-ot-21-dekabrya-2017-g-n-235
7. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК (от 25.12.2017 № 239) [Электронный ресурс] : сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/en/53-normotvorcheskaya/akty/prikazy/1592-prikaz-fstek-rossii-ot-25-dekabrya-2017-g-n-239
8. Об утверждении формы акта проверки, составляемого по итогам проведения государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: Приказ ФСТЭК России (от 11.12.2017 № 229) [Электронный ресурс]: сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/1475-prikaz-fstek-rossii-ot-11-dekabrya-2017-g-n-229
9. Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий: Приказ ФСТЭК России (от 22.12.2017 № 236) [Электронный ресурс] : сайт Федеральной службы по техническому и экспортному контролю: https://fstec.ru/index?id=1607:prikaz-fstek-rossii-ot-22-dekabrya-2017-g-n-236
10. О персональных данных: Федеральный Закон (от 27 июля 2006 г. №152-ФЗ) [Электронный ресурс] : справочная правовая система: http://www.consultant.ru/document/Cons_doc_LAW_61801/

Дополнительная литература:

11. Кудрявцев А.М. Киберустойчивость информационно-телекоммуникационной сети / М.А. Коцыняк, И.А. Кулешов, А.М. Кудрявцев, О.С. Лаутаи. – СПб.: Бостон-спектр, 2015. – 150 с.
12. Чукарин А.В. Бизнес-процессы и информационные технологии в управлении современной инфокоммуникационной компанией / А.В. Чукарин. – М.: Альпина Паблишер. – 2016. - 512 с.

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

1. Справочная правовая система «КонсультантПлюс» – http://www.consultant-plus.ru.
2. Электронная библиотечная система «Университетская библиотека онлайн» – https://biblioclub.ru.
3. Электронная библиотечная система издательства «Лань» – https://e.lanbook.com/
4. Электронный каталог Библиотеки БашГУ – http://www.bashlib.ru/catalogi/
5. www.fstec.ru –сайт ФСТЭК России
6. www.fsb.ru – сайт ФСБ России
7. http://window.edu.ru/ – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
8. http://univertv.ru/video/matematika/ – Открытый образовательный видеопортал UniverTV.ru. Образовательные фильмы на различные темы. Лекции в ведущих

российских и зарубежных вузах. Научная конференция или научно-популярная лекция по интересующему вопросу);

9. www.newlibrary.ru – Новая электронная библиотека;
10. www. edu.ru – Федеральный портал российского образования;
11. www.elibrary.ru – Научная электронная библиотека;
12. www.nehudlit.ru – Электронная библиотека учебных материалов.
13. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
14. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
15. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.

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

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения	
1. ***учебная аудитория для проведения занятий лекционного типа:*** аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус). **2.** ***учебная аудитория для проведения лабораторных работ:*** компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус), Лаборатория систем и сетей передачи данных, сетей и систем передачи	Лекции, практические занятия, лабораторные занятия, курсовое проектирование (выполнение курсовых работ), групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация	**Аудитория № 403** Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия. **Аудитория № 405** Учебная мебель, доска, вокальные радиомикрофоны AKGWMS 40 – 2шт., Интер-ая система со встроенным короткофокусным проекто-ром PrometheanActivBoard 387 RPOMOUNTEST -1 шт., Ком-ер встраиваемый в кафедру INTELCorei3-4150/DDr3 4 Gb/HDD, Экран настенный DraperLumaAV(1:1) 96/96”244*244MV(XT1000E) -1 шт., Настольный интерактивный дисплей , ActivPanel 21S – 1 шт. , Матричный коммутатор сигналов интерфейса HDMICMPRO 4H4H – 1 шт. , Мультимедиа-проектор PanasonicPT-EW640E - 1 шт., Двух-полосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W)(белый) -6 шт., Петличный радиомикрофон AKGWMS45 – 1 шт. , Терминал видео конференц-связи LifeSizeIcon 600 Camera 10xPhone 2ndGeneration – 1 шт., Экран настенный DraperLumaAV(1:1) 96/96”244*244MV (XT1000E) -1 шт. **Аудитория № 413** Учебная мебель, доска, двухполосный	1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные. 2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные. 3. Система

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 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),		настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 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 МА1225 – 1 шт. **Аудитория № 416** Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 418** Учебная мебель, доска, Экран настенный Lumien Master Pikture 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт. **Аудитория № 419** Учебная мебель, Проектор Optoma Ex542 i – 1 шт., Экран настенный Dinon – 1 шт. **Аудитория № 515** Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профес-сиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI CMPRO 4H4H, интер-ая напольная кафедра докладчика, ком-ер встраиваемый в кафедру IN-TEL Core i3-4150/DDr3 4 Gb/HDD 1TB/DVD-RW/Therm altake VL520B1N2E 220W/Win8Pro64, стол, трибуна, кресла секционные последующих рядов с пюпитром. **Аудитория № 516** Учебная мебель, доска, кресла секционные последующих рядов с пюпитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран. **Аудитория № 509** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 608** Учебная мебель, доска, мобильное мультимедийное оборудование. **Аудитория № 609** Учебная мебель, доска, мобильное мультимедийное оборудование.	централизованного тестирования БашГУ (Moodle).GNU General Public License.

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 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).		**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.	

Приложение 1

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

Содержание рабочей программы
дисциплины **Основы безопасности критической информационной инфраструктуры**
на 7 семестр ОФО

Вид работы	Объем дисциплины
Общая трудоемкость дисциплины (ЗЕТ / часов)	3 ЗЕТ / 108 часа
Учебных часов на контактную работу с преподавателем:	55,2
лекций	18
практических/ семинарских	36
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)	25,8
Учебных часов на подготовку к экзамену/зачету/дифференцированному зачету (Контроль)	27

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	ЛР	СРС		
1	2	3	4	5	6	7	8
1	Теоретические аспекты вопроса обеспечения безопасности критической информационной инфраструктуры	4	6		8	Самостоятельное изучение рекомендуемых источников и материалов	Т, ПР
2	Исследование вопроса необходимости обеспечения информационной безопасности организации	4	10		8	Самостоятельное изучение рекомендуемых источников и материалов	Т, ПР
3	Категорирование объекта критической информационной инфраструктуры организации	6	10		10,8	Самостоятельное изучение рекомендуемых источников и материалов	Т, ПР
4	Совершенствование комплексной системы обеспечения информационной безопасности организации	4	10		8	Самостоятельное изучение рекомендуемых источников и материалов	Т, ПР
	Всего	18	36		34,8		

Т - тестирование, ПР - практические работы