

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

Утверждено:  
на заседании кафедры  
протокол № 11 от «20» июня 2019 г.  
Зав. кафедрой *И.С.* / А.С. Исмагилова

Согласовано:  
Председатель УМК института  
*Г.* /Р.А. Гильмутдинова

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)**

Информационно-аналитическая деятельность по обеспечению комплексной безопасности

Б1.В.1.ДВ.03.01 вариативная

программа бакалавриата

Направление подготовки  
10.03.01 Информационная безопасность

профиль подготовки  
Организация и технология защиты информации

Квалификация  
бакалавр

Разработчик (составитель)  
старший преподаватель

/А.М. Махмутов

Дата приема: 2019 г.

Уфа 2019 г.

Составитель: А.М. Махмутов

Рабочая программа дисциплины утверждена на заседании кафедры управления информационной безопасностью протокол №11 от «20» июня 2019 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/

### Список документов и материалов

1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы	4
2. Цель и место дисциплины в структуре образовательной программы	9
3. Содержание рабочей программы (объем дисциплины, типы и виды учебных занятий, учебно-методическое обеспечение самостоятельной работы обучающихся)	9
4. Фонд оценочных средств по дисциплине	10
4.1. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания	10
4.2. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций	20
4.3. Рейтинг-план дисциплины	25
5. Учебно-методическое и информационное обеспечение дисциплины	32
5.1. Перечень основной и дополнительной учебной литературы, необходимой для освоения дисциплины	32
5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины	33
6. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине	34

## 1. Перечень планируемых результатов обучения по дисциплине, соотнесенных с планируемыми результатами освоения образовательной программы

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

Результаты обучения		Формируемая компетенция (с указанием кода)	Примечание
Знания	1. основные понятия информатики; разделы информатики, состав программного обеспечения, файловые системы, технические средства, актуальные характеристики основных периферийных устройств компьютеров, виды операционных систем, историю и тенденции их развития, назначение, состав, функции и возможности автоматизированных справочных систем, информационно-поисковых систем, банков и баз данных, методы организации сбора, обработки, анализа и систематизации статистических данных; теоретические основы цифровой обработки акустических, фото- и видеоматериалов	– способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4)	
	2. основы российской правовой системы и законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ, основные понятия, цели, принципы, сферы применения, объекты, субъекты, правовые основы своей профессиональной деятельности, ее составляющих элементов,	– способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)	

	<p>роль договоров в сфере информационной безопасности; виды юридической ответственности, методы и средства правовой защиты интересов субъектов в сфере информационной безопасности</p>		
	<p>3. средства контроля контента, средства анализа защищенности и средства обнаружения атак для обеспечения безопасности в IP-сетях, средства защиты от несанкционированного доступа, применение межсетевых экранов</p>	<p>– способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)</p>	
	<p>4. нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом, стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, методики анализа рисков информационных систем</p>	<p>– способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7)</p>	
	<p>5. критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов</p>	<p>– способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)</p>	

Умения	1. понимать и применять на практике компьютерные технологии для решения различных задач комплексного и гармонического анализа, использовать программные и аппаратные средства персонального компьютера, администрировать персональный компьютер, проводить сервисные и профилактические работы, осуществлять ввод, обработку, хранение, поиск, передачу и получение информации, работать с использованием автоматизированных справочных информационно-поисковых систем; проектировать базы данных	– способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4)	
	2. ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности, предвидеть юридические опасности и угрозы, связанные с использованием информации, и соблюдать основные правовые требования информационной безопасности, в т.ч. защиты интеллектуальной собственности; предпринимать необходимые меры по восстановлению нарушенных прав	– способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)	
	3. использовать базовые	– способность определять	

	<p>возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность, использовать системы электронного документооборота, работать с информацией в глобальных компьютерных сетях</p>	<p>информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)</p>	
	<p>4. интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных, разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества</p>	<p>– способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7)</p>	
	<p>5. применять отечественные стандарты в области компьютерной безопасности для проектирования, разработки и оценки защищенности компьютерных систем, собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и прочих источниках</p>	<p>– способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)</p>	
<p>Владения (навыки / опыт деятельности)</p>	<p>1. решения практических задач, графическим интерфейсом пользователя, интерфейсом командной строки, стандартными программами,</p>	<p>– способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации (ОПК-4)</p>	

	<p>антивирусными программами, сервисным программным обеспечением операционной системы, навыками настройки компьютерной сети, навыками работы с информацией в корпоративных информационных системах, навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями, навыками автоматизации формирования информационных ресурсов, навыками систематизации, обобщения и анализа данных (в том числе и статистических</p>		
	<p>2. анализа юридических последствий, связанных с использованием информации, опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности,</p>	<p>– способность использовать нормативные правовые акты в профессиональной деятельности (ОПК-5)</p>	
	<p>3. методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам, навыками работы с компьютером как средством защиты информации</p>	<p>– способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты (ОПК-7)</p>	



	4. интерпретацией и обобщения результатов, формулирования рекомендаций и принятия решений, методологией и навыками решения научных и практических задач	– способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений (ПК-7)	
	5. методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов, навыками анализа и интерпретации информации, содержащейся в различных источниках	– способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности (ПК-10)	

## 2. Цель и место дисциплины (модуля) в структуре образовательной программы

Дисциплина «Информационно-аналитическая деятельность по обеспечению комплексной безопасности» относится к дисциплинам вариативной части образовательной программы.

Дисциплина изучается на 3 курсе в 5 семестре.

Цели изучения дисциплины: формирование у специалистов целостного представления об общих закономерностях развития и функционирования систем защиты информации.

Изучение дисциплины базируется на знаниях, умениях и навыках, сформированных в результате освоения студентами предшествующих дисциплин образовательной программы по направлению подготовки 10.03.01 – «Информационная безопасность» профиля «Организация и технология защиты информации»: «Физика», «Информатика».

Освоение дисциплины «Информационно-аналитическая деятельность по обеспечению комплексной безопасности» служит основой для выполнения практических мероприятий по защите информации. Полученные знания, навыки и умения используются при прохождении преддипломной практики и в ходе выполнения выпускной квалификационной работы.

## 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 с указанием этапов их формирования в процессе освоения образовательной программы. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

ОПК-4. Способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: основные понятия и задачи в области информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности	Имеет фрагментарные знания об основных понятиях в области информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности	В целом знает основные понятия и задачи в области информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности, но допускает значительные ошибки	Знает основные понятия и задачи в области информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности, но допускает незначительные ошибки	Демонстрирует целостность знания об основных понятиях и задачах в области информационно-коммуникационных технологий для решения стандартных задач профессиональной деятельности
Второй этап (уровень)	Уметь: работать с офисными программами, проводить поиск информации, осуществлять сбор и анализ данных, необходимых для проведения	Умеет работать с офисными программами, но не способен проводить поиск информации, осуществлять сбор и анализ данных,	Умеет работать с офисными программами, проводить поиск информации, осуществлять сбор и анализ данных, необходимых для	Уверенно работает с офисными программами, проводить поиск информации, осуществлять сбор и анализ данных, необходимых для	Уверенно работает с офисными программами, проводить поиск информации, осуществлять сбор и анализ данных, необходимых для

	конкретных расчетов; обрабатывать массивы данных в соответствии с поставленной задачей.	необходимых для проведения конкретных расчетов; обрабатывать массивы данных в соответствии с поставленной задачей.	проведения конкретных расчетов; но не умеет обрабатывать массивы данных в соответствии с поставленной задачей.	проведения конкретных расчетов; обрабатывать массивы данных в соответствии с поставленной задачей, но допускает незначительные ошибки.	проведения конкретных расчетов; обрабатывать массивы данных в соответствии с поставленной задачей.
Третий этап (уровень)	Владеть: информационно-коммуникационными технологиями с учетом основных требований информационной безопасности.	Не способен выбрать необходимые для работы информационно-коммуникационные технологии.	Владеет способностью выбора информационно-коммуникационными технологиями, но без учета основных требований информационной безопасности	Владеет способностью аргументированного выбора информационно-коммуникационными технологиями, но испытывает незначительные трудности при обеспечении информационной безопасности	Владеет способностью выбора и использования информационно-коммуникационными технологиями с учетом основных требований информационной безопасности

ОПК-5. Способность использовать нормативные правовые акты в профессиональной деятельности

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: Правовые нормы и стандарты по лицензированию	Имеет фрагментарные знания о законодательной базе	Знает основные законодательные акты по защите	Знает основные законодательные акты по защите	Знает основные законодательные акты по защите

	ию в области обеспечения защиты государственной тайны и сертификации средств защиты информации; правовые основы организации защиты государственной тайны и конфиденциальной информации, системы организации бумажного и электронного конфиденциального делопроизводства	обеспечения информации безопасности	информации, однако допускает значительные ошибки при их интерпретации	информации, однако допускает незначительные ошибки при их интерпретации	информации в государственных и частных структурах
Второй этап (уровень)	Уметь: Выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации; Применять на практике методы локальной и комплексной автоматизации и процессов обработки документов в документационной службе; Разрабатывать организационно-распорядитель	Не показывает сформированные умения опираться на законодательную базу, а также разрабатывать организационно-распорядительные документы по защите информации	Умеет выбирать тип необходимых средств для выявления наличия электронных средств перехвата информации, разрабатывать организационно-распорядительные документы по вопросам защиты информации, однако, не может применить на практике.	Способен обосновывать выбор необходимых средств для выявления наличия электронных средств перехвата информации, а также умеет составлять сопровождающую организационно-распорядительную документацию.	Аргументировано обосновывает и представляет необходимость применения конкретного типа средств противодействия перехвату электронных документов; Уметь применять методы защищенной автоматизации и обработки документов

	ьные документы по вопросам защиты информации;				
Третий этап (уровень)	Владеть: Навыками работы с нормативными и правовыми актами и навыками лицензирования в области защиты информации; методами сбора и анализа исходных данных для проектирования систем защиты информации, определение требований, сравнительный анализ подсистем по показателям информационной безопасности	Отсутствуют навыки работы с нормативными правовыми актами и навыками лицензирования в области защиты информации;	В целом владеет навыками работы с нормативными правовыми актами; владеет методами сбора и анализа исходных данных для проектирования систем защиты информации	В целом владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации; методами сбора и анализа исходных данных для проектирования систем защиты информации, но допускает незначительные ошибки при анализе системы безопасности	Владеет навыками работы с нормативными правовыми актами и навыками лицензирования в области защиты информации; может спроектировать систему защиты информации,

ОПК-7. Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: виды и формы информации, подверженно	Имеет фрагментарные знания об основных	В целом знает основные виды и	Знает основные виды и формы	Знает основные виды и формы

	й угрозам; средства защиты от несанкционир ованного доступа; средства для обнаружения атак и анализа защищенност и объекта	видах и формах информации и средств для ее анализа и защиты	формы информации и средства для ее анализа и защиты, но допускает значительны е ошибки	информации и средства для ее анализа и защиты, но допускает незначительн ые ошибки	информации и средства для ее анализа и защиты
Второй этап (уровень)	Уметь: использовать возможности информацион ных систем для обеспечения информацион ной безопасности предприятия; работать с ПК, как со средством защиты информации	Не показывает сформирован ные умения в использовани и возможности информацио нных систем и в работе с ПК, как со средством защиты информации	Ориентирует ся в работе ПК, как со средством защиты информации, но не использует возможности информацио нных систем	Способен использовать возможности информацио нных систем для обеспечения информацио нной безопасности предприятия, но испытывает сложности со связью теории и поставленно й задачей	Уверенно использует возможности информацио нных систем для обеспечения информацио нной безопасности предприятия и работает с ПК, как со средством защиты информации
Третий этап (уровень)	Владеть: методикой определения видов информации; навыками анализа угроз информацион но- вычислительн ым системам и путей их реализации	Не способен определять виды информации, анализироват ь угрозы информацио нно- вычислитель ным системам	В целом владеет навыками определения видов информации; навыками анализа угроз информацио нно- вычислитель ным системам и путей их реализации, но допускает значительны е ошибки	Владеет методикой определения видов информации и навыками анализа угроз информацио нно- вычислитель ным системам, но испытывает незначительн ые трудности при определении путей реализации угроз	Владеет методикой определения видов информации; навыками анализа угроз информацио нно- вычислитель ным системам и путей их реализации

ПК-7. Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: подходы обоснования затрат на информационную безопасность; методы и модели установления зависимости между затратами на защиту информации и уровнем защищенности, нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом; стандарты построения систем информационной безопасности и стандарты оценки степени защиты систем	Фрагментарные представления о подходах к обоснованию затрат на информационную безопасность, Имеет фрагментарные знания о нормативно-правовых документах по обеспечению информационной безопасности в нашей стране и за рубежом; стандартах построения систем информационной безопасности и стандартах оценки степени защиты систем информационной безопасности объектов;	В целом успешные, но не систематические представления о подходах к обоснованию затрат на информационную безопасность, методиках анализа рисков информационных систем; подходах к обоснованию затрат на информационную безопасность, знает большинство нормативно-правовых документов по обеспечению информационной безопасности в нашей стране и за рубежом; стандартов	В целом успешные, но содержащие отдельные пробелы, представления о подходах к обоснованию затрат на информационную безопасность; методах и моделях установления зависимости между затратами на защиту информации и уровнем защищенности, знает нормативно-правовые документы по обеспечению информационной безопасности в нашей стране и за рубежом; стандарты построения систем	Сформированные представления о подходах к обоснованию информационной безопасности; методах и моделях установления зависимости между затратами на защиту информации и уровнем защищенности, свободное знание нормативно-правовых документов по обеспечению информационной безопасности в нашей стране и за рубежом; стандартов построения систем информационной безопасности

	информационной безопасности объектов; методики анализа рисков информационных систем	методиках анализа рисков информационных систем	построения систем информационной безопасности и стандартов оценки степени защиты систем информационной безопасности объектов; методик анализа рисков информационных систем	информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов; методики анализа рисков информационных систем	и стандартов оценки степени защиты систем информационной безопасности объектов; методик анализа рисков информационных систем
Второй этап (уровень)	Уметь: оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; самостоятельно находить нужную информацию по тематике и выбирать необходимые для организации информационные ресурсы и источники знаний в электронной среде; использовать основные методики оценки совокупной	Слабо выраженные способности к работе с данными, использованию основных методик оценки совокупной стоимости владения для подсистемы информационной безопасности; определению зависимости между затратами на ИБ и уровнем защищенности; слабые умения интерпретировать и обобщать данные, формулировать выводы и рекомендации	Умеет работать с данными, оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения, использовать основные методики оценки совокупной стоимости владения для подсистемы информационной безопасности под руководством более квалифицированных работников;	Умеет применять на практике методы обработки данных, использовать основные методики оценки совокупной стоимости владения для подсистемы информационной безопасности; определять зависимость между затратами на ИБ и уровнем защищенности, но испытывает небольшие затруднения в самостоятельной оценке эффективности	Умеет оценивать эффективность управленческих решений и анализировать экономические показатели деятельности подразделения; самостоятельно находить нужную информацию; использовать основные методики оценки совокупной стоимости владения для подсистемы информационной безопасности; определять зависимость между



	стоимости владения для подсистемы информационной безопасности; определять зависимость между затратами на ИБ и уровнем защищенности, интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных, разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	и, применять на практике методы обработки данных, разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	сформированные, но с пробелами умения интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных, разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	управленческих решений и анализе экономических показателей деятельности подразделения, способен интерпретировать и обобщать данные, формулировать выводы и рекомендации на практике методы обработки данных, разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества	затратами на ИБ и уровнем защищенности, способен уверенно интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных, разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества
Третий этап (уровень)	Владеть: навыками определения затрат компании на ИБ, навыками интерпретации и обобщения результатов, формулирования рекомендаций и принятия решений,	Фрагментарные навыки определения затрат компании на ИБ, слабые навыки интерпретации и обобщения результатов, формулирования рекомендаций и принятия	В целом успешные, но не систематические навыки определения затрат компании на ИБ, в целом сформированные навыки интерпретации и обобщения результатов,	В целом успешное, но содержащее отдельные пробелы навыки определения затрат компании на ИБ, хорошие, но с некоторыми пробелами навыки интерпретации	Успешное и систематическое применение навыков определения затрат компании на ИБ, уверенные навыки интерпретации и обобщения результатов,

методологией и навыками решения научных и практических задач	решений, методологией и навыками решения научных и практических задач	формулирования рекомендаций и принятия решений, методологией и навыками решения научных и практических задач	ии и обобщения результатов, формулирования рекомендаций и принятия решений, методологией и навыками решения научных и практических задач	формулирования рекомендаций и принятия решений, методологией и навыками решения научных и практических задач
--	---	--	--	--

ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности.

Этап (уровень) освоения компетенции	Планируемые результаты обучения (показатели достижения заданного уровня освоения компетенций)	Критерии оценивания результатов обучения			
		2 («Не удовлетворительно»)	3 («Удовлетворительно»)	4 («Хорошо»)	5 («Отлично»)
Первый этап (уровень)	Знать: критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов	Имеет фрагментарные знания о критериях оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов	В целом знает основные критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов, но допускает значительные ошибки.	Хорошо знает основные критерии оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов, но допускает незначительные ошибки.	Демонстрирует целостность знаний критериев оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов
Второй этап (уровень)	Уметь: Применять отечественные стандарты в области компьютерно	Умеет использовать отечественные стандарты в области компьютерно	Умеет применять отечественные стандарты в области компьютерно	Умеет применять отечественные стандарты в области компьютерно	Умеет эффективно применять отечественные стандарты в области

	<p>й безопасности для проектирования, разработки и оценки защищенности и компьютерных систем; собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и прочих источниках</p>	<p>й безопасности, но не способен применить их для проектирования, разработки и оценки защищенности и компьютерных систем; не способен собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и прочих источниках</p>	<p>й безопасности для проектирования, разработки и оценки защищенности и компьютерных систем; собирать, анализировать информацию, но не умеет интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и прочих источниках</p>	<p>й безопасности для проектирования, разработки и оценки защищенности и компьютерных систем; собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и прочих источниках, но допускает незначительные ошибки.</p>	<p>компьютерно й безопасности для проектирования, разработки и оценки защищенности и компьютерных систем; собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и прочих источниках</p>
<p>Третий этап (уровень)</p>	<p>Владеть: Методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; навыками анализа и интерпретации информации, содержащейся в различных источниках</p>	<p>Не способен провести проверки защищенности объектов информатизации на соответствие требованиям нормативных документов.</p>	<p>Владеет методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов, но без анализа и интерпретации информации, содержащейся в различных источниках</p>	<p>Владеет методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов, но испытывает незначительные трудности при анализе и интерпретации информации, содержащейся</p>	<p>Владеет методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов; обладает навыками анализа и интерпретации информации, содержащейся в различных источниках</p>

				я в различных источниках	
--	--	--	--	--------------------------------	--

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 оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Этапы освоения	Результаты обучения	Компетенция	Оценочные средства
1-й этап Знания	основных понятий информатики; разделов информатики, состава программного обеспечения, файловых систем, технических средств, актуальных характеристик основных периферийных устройств компьютеров, видов операционных систем, истории и тенденции их развития, назначение, состав, функции и возможности автоматизированных справочных систем, информационно-поисковых систем, банков и баз данных, методы организации сбора, обработки, анализа и систематизации статистических данных; теоретические основы цифровой обработки акустических, фото- и видеоматериалов	ОПК-4: Способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Тестирование, Лабораторное задание, творческое задание
	основ российской правовой системы и	ОПК-5: Способность использовать	Тестирование, Лабораторное задание,

	<p>законодательства, правового статуса личности, организации и деятельности органов государственной власти в РФ, основных понятий, целей, принципов, сферы применения, объекты, субъекты, правовых основ своей профессиональной деятельности, ее составляющих элементов, роли договоров в сфере информационной безопасности; видов юридической ответственности, методов и средств правовой защиты интересов субъектов в сфере информационной безопасности</p>	<p>нормативные правовые акты в профессиональной деятельности</p>	<p>творческое задание</p>
	<p>средств контроля контента, средств анализа защищенности и средств обнаружения атак для обеспечения безопасности в IP-сетях, средств защиты от несанкционированного доступа, применения межсетевых экранов</p>	<p>ОПК-7: Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p>	<p>Тестирование, Лабораторное задание, творческое задание</p>
	<p>нормативно-правовых документов по обеспечению информационной безопасности в нашей стране и за рубежом, стандартов построения систем информационной безопасности и стандарты оценки степени защиты систем информационной безопасности объектов, методики анализа</p>	<p>ПК-7. Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.</p>	<p>Тестирование, Лабораторное задание, творческое задание</p>

	рисков информационных систем		
	критериев оценки уровня информационной безопасности объектов и систем с использованием отечественных стандартов	ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности	Тестирование, Лабораторное задание, творческое задание
2-й этап Умения	понимать и применять на практике компьютерные технологии для решения различных задач комплексного и гармонического анализа, использовать программные и аппаратные средства персонального компьютера, администрировать персональный компьютер, проводить сервисные и профилактические работы, осуществлять ввод, обработку, хранение, поиск, передачу и получение информации, работать с использованием автоматизированных справочных информационно-поисковых систем; проектировать базы данных	ОПК-4: Способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Тестирование, Лабораторное задание, творческое задание
	ориентироваться в нормативно-правовых актах, регламентирующих сферу профессиональной деятельности, и использовать их в своей деятельности, предвидеть юридические опасности	ОПК-5: Способность использовать нормативные правовые акты в профессиональной деятельности	Тестирование, Лабораторное задание, творческое задание

	<p>и угрозы, связанные с использованием информации, и соблюдать основные правовые требования информационной безопасности, в т.ч. защиты интеллектуальной собственности; предпринимать необходимые меры по восстановлению нарушенных прав</p>		
	<p>использовать базовые возможности информационных систем для решения задач фирмы, внедрять компоненты систем предприятия, обеспечивающие информационную безопасность, использовать системы электронного документооборота, работать с информацией в глобальных компьютерных сетях</p>	<p>ОПК-7: Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p>	<p>Тестирование, Лабораторное задание, творческое задание</p>
	<p>интерпретировать и обобщать данные, формулировать выводы и рекомендации, применять на практике методы обработки данных, разрабатывать и реализовывать решения, направленные на поддержку социально-значимых проектов и развитие компьютерного творчества</p>	<p>ПК-7. Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.</p>	<p>Тестирование, Лабораторное задание, творческое задание</p>
	<p>применять отечественные стандарты в области компьютерной безопасности для проектирования, разработки и оценки</p>	<p>ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной</p>	<p>Тестирование, Лабораторное задание, творческое задание</p>

	защищенности компьютерных систем, собирать, анализировать и интерпретировать необходимую информацию, содержащуюся в различных формах отчетности и прочих источниках	безопасности	
3-й этап Владения навыками	навыками решения практических задач, графическим интерфейсом пользователя, интерфейсом командной строки, стандартными программами, антивирусными программами, сервисным программным обеспечением операционной системы, навыками настройки компьютерной сети, навыками работы с информацией в корпоративных информационных системах, навыками поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями, навыками автоматизации формирования информационных ресурсов, навыками систематизации, обобщения и анализа данных (в том числе и статистических	ОПК-4: Способность понимать значение информации в развитии современного общества, применять информационные технологии для поиска и обработки информации	Тестирование, Лабораторное задание, творческое задание
	навыками анализа юридических последствий, связанных с	ОПК-5: Способность использовать нормативные правовые акты в профессиональной	Тестирование, Лабораторное задание, творческое задание



<p>использованием информации, опытом работы с действующими федеральными законами, нормативной и технической информацией, необходимой для профессиональной деятельности,</p>	<p>деятельности</p>	
<p>методикой определения видов и форм информации, подверженной угрозам, анализировать угрозы информационно-вычислительным системам, навыками работы с компьютером как средством защиты информации</p>	<p>ОПК-7: Способность определять информационные ресурсы, подлежащие защите, угрозы безопасности информации и возможные пути их реализации на основе анализа структуры и содержания информационных процессов и особенностей функционирования объекта защиты</p>	<p>Тестирование, Лабораторное задание, творческое задание</p>
<p>интерпретацией и обобщения результатов, формулирования рекомендаций и принятия решений, методологией и навыками решения научных и практических задач</p>	<p>ПК-7. Способность проводить анализ исходных данных для проектирования подсистем и средств обеспечения информационной безопасности и участвовать в проведении технико-экономического обоснования соответствующих проектных решений.</p>	<p>Тестирование, Лабораторное задание, творческое задание</p>
<p>методиками проверки защищенности объектов информатизации на соответствие требованиям нормативных документов, навыками анализа и интерпретации информации, содержащейся в различных источниках</p>	<p>ПК-10. Способность проводить анализ информационной безопасности объектов и систем на соответствие требованиям стандартов в области информационной безопасности</p>	<p>Тестирование, Лабораторное задание, творческое задание</p>

### 4.3. Рейтинг-план дисциплины

Рейтинг–план дисциплины представлен в приложении 2

#### Экзамен

Структура экзаменационного билета: экзаменационный билет состоит из двух вопросов, отражающих соответственно материал первого и второго модуля.

#### Типовые экзаменационные материалы

1. Планирование ИАДКБ. Этапы ИАДКБ.
2. Системный подход в ИАДКБ.
3. Анализ модельной информации.
4. Определение основных категорий и понятий.
5. Определение критериев оценки.
6. Сравнительная характеристика. Количественные и качественные характеристики.
7. Методика анализа информативности источников.
8. Проблема активной фильтрации сообщений. Качественные характеристики информации.
9. Режимы восприятия информации. Атрибуция сообщений.
10. Оценка полноты, непротиворечивости и достоверности информации.
11. Технология создания аналитических документов.
12. Критерии, параметры ограничения логической непротиворечивости и достоверности информации.
13. Аналитический обзор и аналитическая записка: принципы составления.
14. Информационная справка: принципы составления.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИСТОРИИ И ГОСУДАРСТВЕННОГО УПРАВЛЕНИЯ

---

Направление подготовки 10.03.01 Информационная безопасность

Дисциплина Информационно-аналитическая деятельность по обеспечению комплексной безопасности

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

- 1 Планирование ИАДКБ. Этапы ИАДКБ.
- 2 Режимы восприятия информации. Атрибуция сообщений.

Зав. кафедрой управления  
информационной безопасностью

А.С. Исмагилова

Кафедра управления информационной безопасностью

---

Устанавливается следующая градация перевода оценки из многобалльной в четырехбалльную:

Экзамены:

- отлично – от 80 до 110 баллов (включая 10 поощрительных баллов),
- хорошо – от 60 до 79 баллов,
- удовлетворительно – от 45 до 59 баллов,
- неудовлетворительно – менее 45 баллов.

Критерии оценивания результатов экзамена для ОФО:

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.

- 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.

- 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.

- 1-10 баллов выставляется студенту, если 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

### Тестирование

1. К принципам обеспечения безопасности относится:
  - а) согласованность;
  - б) взаимная ответственность личности, общества и государства;
  - в) децентрализации и демократизм.
2. Совокупность условий и факторов, создающих опасность жизненно важным интересам личности, общества и государства:
  - а) угроза информационной безопасности;
  - б) предполагаемые действия иностранных государств;
  - в) деятельность иностранных разведок.
3. Не являются видами угроз информационной безопасности:
  - а) внутренние угрозы;
  - б) внешние угрозы;
  - в) значительные угрозы.
4. Не являются видами угроз информационной безопасности:
  - а) угрозы военные;
  - б) угрозы потенциальные;
  - в) угрозы реальные.
5. К методам обеспечения информационной безопасности Российской Федерации относятся:
  - а) правовые;
  - б) неправовые;
  - в) легальные.
6. К методам обеспечения информационной безопасности Российской Федерации относятся:
  - а) методы принуждения;
  - б) организационно-технические;
  - в) секретные.
7. К методам обеспечения информационной безопасности Российской Федерации относятся:
  - а) оперативные;
  - б) конструктивные;
  - в) экономические.
8. Сфера деятельности субъектов, связанная с созданием, преобразованием и потреблением информации это:
  - а) сфера хранения информации;
  - б) информационная сфера;
  - в) сфера государственного регулирования информации.

### Критерии оценивания теста

В комплекте тестов 25 вопросов,  
за один правильный ответ ставится 0.4 балла.  
За тест максимальный балл 10 баллов

## Лабораторное задание

Определите название фирмы, выберите вид и область деятельности из перечисленных:

Варианты:

0. факультет университета;
1. филиал банка;
2. небольшое торговое предприятие;
3. поликлиника;
4. больница;
5. железнодорожная станция;
6. школа;
7. библиотека;
8. юридическая фирма;
9. фирма по разработке программного обеспечения.

Составьте план мероприятий по защите информации. Укажите перечень внутрифирменных документов, которые будут использоваться в целях правовой защиты секретов вашей фирмы. Составьте перечень сведений ограниченного распространения вашей организации.

Отчет о выполненной работе оформляется в соответствии с общепринятыми требованиями и предоставляется в виде распечатки контрольного листа из файла.

Критерии и методика оценивания:

- 1 балл выставляется студенту, если работа выполнена, но без заключения;
- 2 балла выставляется студенту, если работа выполнена, но без полноценного заключения;
- 3 балла выставляется студенту, если работа выполнена, имеется полноценное заключение.

### Защита лабораторной работы

Проводится в форме устного опроса после выполнения работы.

Критерии и методика оценивания:

- 0 баллов выставляется студенту, если он не владеет содержанием практической работы;
- 1 балл выставляется студенту, если он частично владеет содержанием работы;
- 2 балла выставляется студенту, если он владеет содержанием работы, но не может объяснить полученные результаты;
- 3 балла выставляется студенту, если он владеет содержанием работы, может объяснить полученные результаты.

### Творческое задание (презентация, доклад)

Выполняется по результатам изучения темы дисциплины с целью дополнения практического материала.

Доклад представляет собой самостоятельное публичное выступление студента по представлению полученных результатов решения определенных учебно-исследовательских или научных задач. Доклад готовится в письменной форме с соблюдением основных требований к работам такого уровня. В докладе раскрываются теоретические основы исследуемой темы, характеризуется объект исследования, выделяются основные управленческие проблемы и пути их решения.

1. Состав и классификация защищаемой информации;
2. Правовые особенности взаимодействия субъектов на рынке информации.
3. Основные методы определения затрат на информационную безопасность.
4. Принципы и методы защиты информации.
5. Правовое обеспечение информационной безопасности. Российские документы по защите информации. Организационное обеспечение информационной безопасности
6. Законодательные и нормативные акты РФ в области защиты информации.
7. Основные задачи подразделения обеспечения безопасности информационных технологий.
8. Общие правила обеспечения безопасности информационных технологий при работе сотрудников с ресурсами автоматизированной системы.
9. Значимые IT-достижения и перспективы информатизации юридической деятельности.
10. Дать определение нижестоящим понятиям:
  - «информатизация»;
  - «информационные технологии»;
  - «информационные технологии в юридической деятельности».
11. Охарактеризовать возможности методов обработки информации, границ их применения;
12. Оценивание точности и достоверности полученной информации;
13. Установление влияния факторов на достоверность полученной информации (при ее поиске);
14. Определение объемов хранимой информации;
15. Анализ и оценка угроз информационной безопасности;
16. Определение размера целесообразных затрат на обеспечение информационной безопасности.
17. Экономическая оценка объектов интеллектуальной собственности, а также анализ и оценка предпринимательских рисков;
18. Осуществление поиска наиболее эффективных путей обработки информации и (или) ее управления.
19. Проводить анализ основных количественных и качественных метрик, используемых в области информационной безопасности.
20. Регламентация процессов разработки, испытания, опытной эксплуатации, внедрения и сопровождения задач. Взаимодействие подразделений на этапах проектирования, разработки, испытания и внедрения новых автоматизированных подсистем.
21. Оценка политик безопасности .
22. Рекомендации по тестированию. Цель, методы и порядок проведения тестирования. Проверка реальных условий размещения и использования оборудования. Тестовые испытания функций защиты от НСД и защиты от утечки по техническим каналам. Моделирование действий злоумышленника (“взлом” защиты информации).
23. Определение требований к защите и категорирование ресурсов.
24. Проведение обследований подсистем, инвентаризация, категорирование и документирование защищаемых ресурсов автоматизированных систем.
25. Составление должностной инструкции.
26. Организация поиска и использование оперативной информации о новых уязвимостях в системном и прикладном программном обеспечении, а также других актуальных для обеспечения информационной безопасности данных.
27. Найти на сайте ИПС «Законодательство России» (<http://pravo.fso.gov.ru/ips.html>) федеральный закон «об оперативно-розыскной деятельности».
28. Определите виды информации:
  1. Агентурное сообщение о работе незаконной лаборатории по изготовлению наркотиков
  2. Законопроект

3. Следы крови на месте преступления
4. Видеозапись разбойного нападения с камеры наблюдения
5. Видеозапись судебного заседания
6. Договор дарения
7. Нарушение соглашения пользованием Интернет-ресурса

#### Критерии оценки доклада

Показатель оценки	Распределение баллов
Соответствие содержания доклада заявленной теме, поставленным целям и задачам	0,5
Логичность и последовательность в изложении материала	0,5
Привлечение актуальных нормативных актов и современной научной литературы	1
Степень обоснованности аргументов и обобщений (полнота, глубина, всесторонность раскрытия темы, корректность аргументации и системы доказательств, характер и достоверность примеров, наличие знаний интегрированного характера, способность к обобщению)	1
Самостоятельность изучения и анализа материала	1
Использование демонстрационных материалов (наличие и качество презентации)	1
<b>ИТОГО</b>	<b>5</b>

Подготовленная и оформленная в соответствии с требованиями работа (презентация, доклад) оценивается преподавателем по следующим критериям:

- уровень эрудированности автора по изученной теме (знание автором состояния изучаемой проблематики, цитирование источников, в т.ч. НПА);
- логичность подачи материала, грамотность автора;
- соответствие работы всем стандартным требованиям к оформлению;
- знания и умения на уровне требований стандарта данной дисциплины: знание фактического материала, усвоение общих понятий и идей.

- 0 баллов выставляется студенту, если работа не соответствует критериям;
- 1 балл выставляется студенту, если работа частично соответствует критериям;
- 3 балла выставляется студенту, если работа соответствует критериям, но отсутствует логичность изложения информации;
- 5 баллов выставляется студенту, если работа полностью соответствует критериям.

### **5. Учебно-методическое и информационное обеспечение дисциплины**

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

##### **Основная литература:**

1. Малюк, А.А. Защита информации в информационном обществе : учебное пособие / А.А. Малюк. - Москва : Горячая линия-Телеком, 2015. - 229 с. : ил., схем., табл. -

Библиогр. в кн. - ISBN 978-5-9912-0481-1 ; То же [Электронный ресурс]. -

URL: <http://biblioclub.ru/index.php?page=book&id=457170>

2. Коваленко, Ю.И. Правовой режим лицензирования и сертификации в сфере информационной безопасности : учебное пособие / Ю.И. Коваленко. - Москва : Горячая линия - Телеком, 2012. - 140 с. : ил. - Библиогр. в кн. - ISBN 978-5-9912-0261-9 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=253538>

#### **Дополнительная литература**

3. Аверченков, В.И. Аудит информационной безопасности : учебное пособие для вузов / В.И. Аверченков. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 269 с. - Библиогр. в кн. - ISBN 978-5-9765-1256-6 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=93245>
4. Аверченков, В.И. Служба защиты информации: организация и управление : учебное пособие для вузов / В.И. Аверченков, М.Ю. Рытов. - 3-е изд., стер. - Москва : Издательство «Флинта», 2016. - 186 с. - Библиогр. в кн. - ISBN 978-5-9765-1271-9 ; То же [Электронный ресурс]. - URL: <http://biblioclub.ru/index.php?page=book&id=93356>
5. Шишкин, В.В. МЕТОДИКА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. [Электронный ресурс] / В.В. Шишкин, Н.К. Юрков, Н.Ж. Мусин. — Электрон. дан. // Надежность и качество сложных систем. — 2013. — № 4. — С. 9-13. — Режим доступа: <http://e.lanbook.com/journal/issue/298784> — Загл. с экрана.

#### **5.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет» и программного обеспечения, необходимых для освоения дисциплины**

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/catalog/>
5. <http://window.edu.ru/> – Наиболее обширная электронная база учебников и методических материалов на сайте информационной системы «Единое окно доступа к образовательным ресурсам»;
6. <http://univertv.ru/video> – 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);
7. [www.newlibrary.ru](http://www.newlibrary.ru) – Новая электронная библиотека;
8. [www.edu.ru](http://www.edu.ru) – Федеральный портал российского образования;
9. [www.elibrary.ru](http://www.elibrary.ru) – Научная электронная библиотека;
10. [www.nehdilit.ru](http://www.nehdilit.ru) – Электронная библиотека учебных материалов.
11. Windows 8 Russian Russian OLP NL Academic Edition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.
12. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.
13. Система централизованного тестирования БашГУ (Moodle).GNU General Public License.



**6. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)**

Наименование специализированных аудиторий, кабинетов, лабораторий	Вид занятий	Наименование оборудования, программного обеспечения	
<p><b>1. учебная аудитория для проведения занятий лекционного типа:</b> аудитория № 403 (гуманитарный корпус), аудитория № 405 (гуманитарный корпус), аудитория № 413 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 515 (гуманитарный корпус), аудитория № 516 (гуманитарный корпус).</p> <p><b>2. учебная аудитория для проведения лабораторных работ:</b> Лаборатория полигон технической защиты информации № 508 (гуманитарный корпус), компьютерный класс, аудитория 404 (гуманитарный корпус), аудитория 420 (гуманитарный корпус).</p> <p><b>3. учебная аудитория для проведения занятий семинарского типа:</b> аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус).</p>	<p>Лекции, практические занятия, лабораторные занятия, групповые и индивидуальные консультации, текущий контроль, промежуточная аттестация</p>	<p align="center"><b>Аудитория № 403</b> Учебная мебель, доска, Мультимедийный-проектор Panasonic PT-LB78VE – 1 шт., Экран настенный Classic Norma 244*183 – 1 шт., учебно-наглядные пособия.</p> <p align="center"><b>Аудитория № 405</b> 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.</p> <p align="center"><b>Аудитория № 413</b> Учебная мебель, доска, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 6 шт., Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p align="center"><b>Аудитория № 415</b> Учебная мебель, двухполосный настенный громкоговоритель 20Вт/100В цвет белый(MASK4T-W) – 2 шт., Интерактивная доска SMART с проектором V25, Микшер-усилитель 120Вт АРАРТ МА1225 – 1 шт.</p> <p align="center"><b>Аудитория № 416</b> Учебная мебель, доска, проектор Optoma Ex542 i- 1 шт., Экран настенный Dinon – 1 шт.</p> <p align="center"><b>Аудитория № 418</b> Учебная мебель, доска, Экран настенный Lumien Master Piktura 153*203 Matte White Fiber Clas(белый корпус) – 1 шт., Проектор Optoma Ex542 i - 1 шт.</p> <p align="center"><b>Аудитория № 419</b> Учебная мебель, Проектор Optoma Ex542</p>	<p>1. Windows 8 Russian Russian OLP NL AcademicEdition и Windows Professional 8 Russian Upgrade OLP NL Academic Edition. Договор №104 от 17.06.2013 г. Лицензии бессрочные.</p> <p>2. Microsoft Office Standard 2013 Russian OLP NL Academic Edition. Договор №114 от 12.11.2014 г. Лицензии бессрочные.</p> <p>3. Система централизованного тестирования БашГУ (Moodle).GNU General Public License..</p>

<p><b>4. учебная аудитория для проведения групповых и индивидуальных консультаций:</b> аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).</p> <p><b>5. учебная аудитория для текущего контроля и промежуточной аттестации:</b> аудитория № 403 (гуманитарный корпус), аудитория № 415 (гуманитарный корпус), аудитория № 416 (гуманитарный корпус), аудитория № 418 (гуманитарный корпус), аудитория № 419 (гуманитарный корпус), аудитория № 509 (гуманитарный корпус), аудитория № 608 (гуманитарный корпус), аудитория № 609 (гуманитарный корпус), аудитория № 610 (гуманитарный корпус), компьютерный класс аудитория № 404 (гуманитарный корпус), компьютерный класс аудитория № 420 (гуманитарный корпус).</p> <p><b>6. помещения для самостоятельной работы:</b> читальный зал библиотеки аудитория 402 (гуманитарный корпус), аудитория № 613 (гуманитарный корпус).</p> <p><b>7.помещение для хранения</b></p>		<p>i – 1 шт., Экран настенный Dinon – 1 шт.</p> <p><b>Аудитория № 515</b> Учебная мебель, доска, терминал видео конференц-связи LifeSize Icon 600-камера, интер-ая система со встроенным короткофокусным проектором Promethean ActivBoard 387 RPO MOUNT EST, профессиональный LCD дисплей Flame 42ST, настольный интерактивный дисплей SMART Podium SP518 с ПО SMART Notebook, матричный коммутатор сигналов интерфейса HDMI SMPRO 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 попитром.</p> <p><b>Аудитория № 516</b> Учебная мебель, доска, кресла секционные последующих рядов с попитром, мобильное мультимедийное оборудование: проектор ASK Proxima, ноутбук HP, экран.</p> <p><b>Аудитория № 509</b> Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p><b>Аудитория № 608</b> Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p><b>Аудитория № 609</b> Учебная мебель, доска, мобильное мультимедийное оборудование.</p> <p><b>Аудитория № 610</b> Учебная мебель, доска, учебно-наглядные пособия, LED Телевизор TCLL55P6 USBLACK – 1 шт., кронштейн для телевизора NBP 5 – 1 шт., Кабель HDMI (m)-HDH(m)ver14,10м.</p> <p><b>Аудитория № 613</b> Учебная мебель, доска, моноблок стационарный – 15 шт.</p> <p><b>Компьютерный класс аудитория № 420</b> Учебная мебель, моноблоки стационарные 15 шт.</p> <p><b>Компьютерный класс аудитория № 404</b> Учебная мебель, компьютеры -15 штук.</p> <p><b>Аудитория 402 читальный зал библиотеки</b> Учебная мебель, доска, компьютеры в комплекте (5 шт.): монитор Samsung, системный блок Asus, клавиатура, мышь, стеллажи, шкафы картотечные, комбинированные.</p> <p><b>Лаборатория полигон технической защиты информации № 508</b> Учебная мебель, учебно-наглядные пособия, аудиторная доска трехсекционная, плакаты с тематикой технической защиты информации, комплекс мониторинга WiFi сетей</p>	
--	--	---	--

<p><i>и профилактического обслуживания учебного оборудования:</i> аудитория № 523 (гуманитарный корпус).</p>		<p>"Зодиак П", универсальный ком-плект инструментов для проведения работ по специальным проверкам и специальным обследованиям  Калейдоскоп-П2, многофункциональный поисковый прибор ST-031M "Пиранья", нелинейный локатор «Лорнет», анализатор электромагнитного поля "Кордон".</p> <p><b>Аудитория № 523</b>  Шкаф-стеллаж – 4 шт., стол-1 шт., стул – 2 шт.</p>	
--	--	---	--

## Приложение 1

МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ  
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ  
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ  
«БАШКИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

### СОДЕРЖАНИЕ РАБОЧЕЙ ПРОГРАММЫ

дисциплины Информационно-аналитическая деятельность по обеспечению комплексной  
безопасности  
на 5 семестр

Вид работы	Объем дисциплины
	Очная форма обучения
Общая трудоемкость дисциплины (ЗЕТ / часов)	4 ЗЕТ / 144 часа
Учебных часов на контактную работу с преподавателем:	73,2
лекций	18
практических / семинарских	36
лабораторных	18
контроль самостоятельной работы (КСР)	
форма контактной работы (ФКР)	
Других (групповая, индивидуальная консультация и иные виды учебной деятельности, предусматривающие работу обучающихся с преподавателем)	1,2
Учебных часов на самостоятельную работу обучающихся, включая подготовку к экзамену	45 25,8

Форма контроля  
Экзамен 5 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 / Сем	ЛР	СРС			
1	2	4	5	6	7	8	9	10
Модуль 1. Основные принципы аналитической деятельности								
1	Цели, задачи, объект, предмет информационно-аналитической деятельности комплексной безопасности (далее – ИАДКБКБ). Специфика ИАДКБ. Терминология. Особенности развития ИАДКБ в России. Основные принципы аналитической деятельности. Понятие информационно-	2	4	2	4	1-5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Тестирование, Лабораторное задание, творческое задание

	аналитических технологий.							
2	Планирование ИАДКБ. Этапы ИАДКБ. Системный подход в ИАДКБ.	2	4	2	4	1-5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Тестирование, Лабораторное задание, творческое задание
3	Анализ модельной информации. Определение основных категорий и понятий. Выработка рабочей гипотезы. Конкретизация цели и задач исследования.	2	4	2	4	1-5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Тестирование, Лабораторное задание, творческое задание
4	Поиск, отбор, экспресс-анализ первичных данных. Оптимизация поиска ресурсов удаленного доступа. Оптимизация поиска ресурсов	2	4	2	4	1-5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Тестирование, Лабораторное задание, творческое задание

	удаленного доступа							
5	Понятийный каркас и структурно-функциональная организация информационно-аналитических технологий.	2	4	2	4	1-5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Тестирование, Лабораторное задание, творческое задание
Модуль 2. Системный подход в ИАДКБ								
1	Анализ модельной информации. Определение основных категорий и понятий. Определение критериев оценки. Сравнительная характеристика. Количественные и качественные характеристики.	2	4	2	4	1-5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-источников.	Тестирование, Лабораторное задание, творческое задание
2	Проблема активной фильтрации сообщений. Качественные характеристики	2	4	2	4	1-5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет-	Тестирование, Лабораторное задание, творческое задание

	информации. Режимы восприятия информации. Атрибуция сообщений.						источников.	
3	Критерии, параметры ограничения логической непротиворечиво сти и достоверности информации.	2	4	2	4	1-5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет- источников.	Тестирование, Лабораторное задание, творческое задание
4	Аналитический обзор и аналитическая записка: принципы составления. Информационная справка: принципы составления. Перспективы становления информационно- аналитической деятельности в сфере информационной безопасности.	2	4	2	5	1-5	Самостоятельное изучение рекомендуемой основной и дополнительной литературы, интернет- источников.	Тестирование, Лабораторное задание, творческое задание



	итого	18	36	18	45			
--	-------	----	----	----	----	--	--	--

Приложение 2  
**Рейтинг – план дисциплины**  
**Информационно-аналитическая деятельность по обеспечению комплексной безопасности**

Направление подготовки 10.03.01 Информационная безопасность  
 Курс 3, семестр 5

Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
			Минимальный	Максимальный
<b>Модуль 1</b>				
Текущий контроль				
1. Аудиторная работа	1	5	0	5
2. Лабораторное задание	3	5	0	15
Рубежный контроль				
1. Тестовые задания	0,4	25	0	10
2. Творческое задание	1	5	0	5
Всего				
<b>Модуль 2</b>				
Текущий контроль			0	
1. Аудиторная работа	1	5	0	5
2. Лабораторное задание	3	5	0	15
Рубежный контроль				
1. Творческое задание	1	5	0	5
2. Тестовые задания	0,4	25	0	10
Всего				
<b>Поощрительные баллы</b>				
1. Студенческая олимпиада			0	3
2. Публикация статей			0	3
3. Участие в конференции			0	4
Всего				10
<b>Посещаемость (баллы вычитаются из общей суммы набранных баллов)</b>				
1. Посещение лекционных занятий				-6
2. Посещение практических занятий				-10
<b>Итоговый контроль</b>				
Экзамен			0	30